Πανεπιστήμιο Αιγαίου

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Διπλωματική εργασία

Διδάσκων / Επιβλέπων: Κρητικός Κυριάκος

Μέλος: Καμπουράκης Γεώργιος

Μέλος: Κωνσταντίνου Ελισάβετ

Επισκόπηση της χρήσης του Blockchain στον υπολογισμό στην ομίχλη και στις άκρες του δικτύου.

3212017094 Κυβέρης Λουκάς

Σάμος, Καρλόβασι, 20/03/2026

Περίληψη

Η παρούσα εργασία εξετάζει ολοκληρωμένα τον τρόπο με τον οποίο η τεχνολογία blockchain μπορεί να συμβάλει στην αντιμετώπιση ζητημάτων ασφάλειας και ιδιωτικότητας στον ομιχλώδη υπολογισμό (fog computing) και στον υπολογισμό στις ακμές του δικτύου (edge computing). Αρχικά παρουσιάζονται αναλυτικά οι βασικές αρχές, τα χαρακτηριστικά, η αρχιτεκτονική και οι εφαρμογές των τριών αυτών τεχνολογιών, καθώς και τα προβλήματα που προκύπτουν στο επίπεδο της ασφάλειας και της προστασίας δεδομένων σε κατανεμημένα περιβάλλοντα χαμηλής καθυστέρησης (latency). Μέσα από μια συστηματική βιβλιογραφική ανασκόπηση αναδεικνύονται οι τρωτότητες και οι επιθέσεις που επηρεάζουν τα fog και edge περιβάλλοντα, καθώς και οι ιδιαίτερες προκλήσεις που σχετίζονται με την κλιμακωσιμότητα (scalability), την ενεργειακή κατανάλωση, την αποθήκευση και την ιδιωτικότητα. Στη συνέχεια διερευνάται ο ρόλος του blockchain ως μια τεχνολογία ενίσχυσης της ακεραιότητας, της ανιχνευσιμότητας και της κατανεμημένης εμπιστοσύνης των δεδομένων. Παρουσιάζονται οι βασικοί τρόποι με τους οποίους το blockchain, τα έξυπνα συμβόλαια, η ελαφριά (lightweight) κρυπτογράφηση και η διαφορική ιδιωτικότητα (differential privacy) καθώς και άλλες συνοδευτικές τεχνολογίες, όπως οι αποδείξεις μηδενικής γνώσης (Zero-Knowledge Proofs), οι τεχνικές ψευδωνυμοποίησης και ανωνυμοποίησης, οι μηχανισμοί data masking, καθώς και ελαφριά σχήματα αυθεντικοποίησης και ελέγχου πρόσβασης, μπορούν να ενισχύσουν την προστασία των δεδομένων και να υποστηρίξουν ασφαλή και αποδοτική λειτουργία σε περιβάλλοντα fog και edge. Τέλος, η εργασία αναδεικνύει τις εναπομένουσες προκλήσεις, καθώς και τις μελλοντικές ερευνητικές κατευθύνσεις αντιμετώπισης των προκλήσεων αυτών, με στόχο την ανάπτυξη πιο ανθεκτικών, κλιμακούμενων και αξιόπιστων αποκεντρωμένων υπολογιστικών υποδομών.

Λέξεις-κλειδιά: Blockchain, Ομιχλώδης Υπολογισμός, Υπολογισμός στις Ακμές του Δικτύου, Ασφάλεια Δεδομένων, Ιδιωτικότητα, Έξυπνα Συμβόλαια, Κρυπτογραφία Χαμηλού Κόστους, Διαφορική Ιδιωτικότητα, Κλιμακωσιμότητα, Επιθέσεις 51%, Αποκεντρωμένη Εμπιστοσύνη, Κατανεμημένα Συστήματα.

Abstract

This thesis provides a comprehensive study of how blockchain technology can contribute to addressing security and privacy issues in fog computing and edge computing environments. Initially, the fundamental principles, characteristics, architectures, and application domains of these three technologies are presented, along with the security and data protection challenges that arise in distributed low-latency environments. Through a systematic literature review, the vulnerabilities and attacks affecting fog and edge infrastructures are analyzed, as well as key challenges related to scalability, energy consumption, storage, and privacy.

The role of blockchain is then investigated as a technology that enhances data integrity, traceability, and decentralized trust. The study examines how blockchain, smart contracts, lightweight cryptography, and differential privacy, together with complementary technologies such as Zero-Knowledge Proofs, pseudonymization and anonymization techniques, data masking mechanisms, and lightweight authentication and access control schemes, can strengthen data protection and support secure and efficient operation in fog and edge environments.

Finally, the thesis highlights the remaining challenges and outlines future research directions aimed at developing more resilient, scalable, and reliable decentralized computing infrastructures.

Keywords:
Blockchain, Fog Computing, Edge Computing, Data Security, Privacy, Smart Contracts, Lightweight Cryptography, Differential Privacy, Scalability, 51% Attacks, Decentralized Trust, Distributed Systems.

Περιεχόμενα

1. Εισαγωγή 11
1.1 Τεχνολογίες Blockchain, Fog & Edge Computing 11
1.2 Συνεισφορά της Διπλωματικής Εργασίας 13
1.2.1 Προσδιορισμός Ερευνητικού Κενού στον Συνδυασμό Blockchain με Fog και Edge Computing 13
1.2.2 Σκοπός και Στόχοι της Έρευνας 13
1.2.3 Αναδυόμενες Καινοτομίες & Καινοτόμες Προσεγγίσεις 13
1.2.4 Αναμενόμενα Οφέλη 14
1.2.5 Προτάσεις για Μελλοντική Έρευνα 14
1.3 Δομή της Αναφοράς της Διπλωματικής 14
2. Υπόβαθρο 16
2.1 Blockchain 16
2.1.1 Ορισμοί Βασικών Εννοιών του Blockchain 16
2.1.2 Είδη Blockchain 18
2.1.3 Χαρακτηριστικά & Οφέλη του Blockchain 20
2.1.4 Αρχιτεκτονική Blockchain 22
2.1.5 Αρχιτεκτονικές Προκλήσεις και Μελλοντικές Ευκαιρίες 26
2.1.6 Λειτουργικοί Ρόλοι Κόμβων στο Blockchain 28
2.1.7 Εφαρμογές και Μελέτες Περίπτωσης 29
2.1.8 Διαδικασία Επικύρωσης και Ροή Συναλλαγών στο Blockchain 33
2.2. Τι είναι ο Ομιχλώδης Υπολογισμός (Fog Computing) 34
2.2.1 Ορισμός 34
2.2.2 Χαρακτηριστικά και Πλεονεκτήματα του Fog Computing 34
2.2.3 Αρχιτεκτονική του Fog Computing 38
2.2.4 Εφαρμογές του Fog Computing 41
2.3 Τι είναι ο Υπολογισμός στις Ακμές του Δικτύου (Edge Computing) 44
2.3.1 Ορισμός 45
2.3.2 Χαρακτηριστικά και Πλεονεκτήματα του Edge Computing 46
2.3.3 Αρχιτεκτονική του Edge Computing 52
2.3.4 Εφαρμογές του Edge Computing 54
2.4 Συγκριτική Ανάλυση Fog και Edge Computing 56
2.4.1 Θέση Επεξεργασίας και Αρχιτεκτονική Διαφοροποίηση 57

2.4.2 Καθυστέρηση, Απόδοση και Διαχείριση Πόρων 58
2.4.3 Κλιμάκωση και Υποστήριξη Πολλαπλών Συσκευών 58
2.4.4 Σχέση με το Υπολογιστικό Νέφος 58
2.4.5 Συνοπτική Σύγκριση Fog και Edge Computing 59
3. Μεθοδολογία Ανασκόπησης 60
3.1. Κύρια Ερευνητικά Ερωτήματα..... 60
3.2. Πηγές & Τρόποι Αναζήτησης Άρθρων 61
3.3. Φιλτράρισμα Άρθρων 64
3.4. Στατιστική Επισκόπηση της Διαδικασίας Επιλογής Βιβλιογραφίας 66
4. Ζητήματα Ασφάλειας και Ιδιωτικότητας στο Fog και Edge Computing 71
4.1. Ζητήματα ασφάλειας 71
4.1.1 Τρωτότητες (Vulnerabilities)..... 71
4.1.2 Επιθέσεις (Attacks)..... 78
4.2. Ζητήματα Ιδιωτικότητας..... 91
4.2.1 Τρωτότητες Ιδιωτικότητας (Privacy vulnerabilities) 92
4.2.2 Επιθέσεις Παραβίασης Ιδιωτικότητας (Privacy Attacks) 96
4.3. Σχετικές Προκλήσεις & Λύσεις στο Fog και στο Edge Computing..... 98
5. Αντιμετώπιση των Ζητημάτων στο Fog & Edge Computing με τη Χρήση του Blockchain 104
5.1. Ο Ρόλος του Blockchain στην Ασφάλεια του Fog & Edge Computing.....104
5.2. Ο Ρόλος του Blockchain στη Διατήρηση της Ιδιωτικότητας του Fog & Edge Computing.....108
6. Προκλήσεις και Ερευνητικές Κατευθύνσεις Σχετιζόμενες με την Εφαρμογή του Blockchain σε Fog/Edge Περιβάλλοντα 118
6.1 Προκλήσεις Απόδοσης & Κατανάλωσης Πόρων.....121
6.1.1. Περιορισμένος ρυθμός διεκπεραίωσης συναλλαγών (throughput) 122
6.1.2. Ζητήματα Καθυστέρησης (latency) 124
6.1.3. Υψηλή Κατανάλωση Ενέργειας.....128
6.1.4. Αυξανόμενες Απαιτήσεις Αποθήκευσης 132
6.2. Προκλήσεις Ασφάλειας και Ιδιωτικότητας.....136
6.2.1. Ευπάθειες σε Επίθεση 51% (51% Attack) 136
6.2.2. Κενά σε έξυπνα συμβόλαια (smart contract vulnerabilities) 140
6.2.3. Ζητήματα Ιδιωτικότητας Συναλλαγών.....144
6.2.4. Κίνδυνοι από Κβαντικούς Υπολογιστές.....147

7. Συμπεράσματα & Επίλογος 150
7.1. Συνεισφορά της Διπλωματικής και Οφέλη 150
7.2. Εμπειρία που Αποκομίστηκε από την Ακπόνηση της Διπλωματικής 151
7.3. Βασικά Συμπεράσματα από τις Αναλύσεις 151
7.4. Ερευνητικές Κατευθύνσεις και Τελική Αποτίμηση 152
8. Βιβλιογραφία.....153

Λίστα Εικόνων

Εικόνα 1: Απεικόνιση επικύρωσης μια συναλλαγής σε μια αλυσίδα blockchain [12]. 16
Εικόνα 2: Αρχιτεκτονική του fog computing [13]. 34
Εικόνα 3: Αρχιτεκτονική του edge computing [14] [15] 44
Εικόνα 4: Overall picture of cloud computing [16]. 45
Εικόνα 5: Η αρχιτεκτονική του edge computing 52
Εικόνα 6: Κατανομή επιλεγμένων πηγών ανά είδος δημοσίευσης 67
Εικόνα 7: Κατανομή επιλεγμένων πηγών ανά είδος εκδότη/πλατφόρμα 68
Εικόνα 8: Κατανομή επιλεγμένων πηγών ανά έτος δημοσίευσης 69
Εικόνα 9: Τρωτότητες σε περιβάλλοντα ομίχλης και ακμών 77
Εικόνα 10: Επιθέσεις σε fog/edge περιβάλλοντα 90

Λίστα Πινάκων

Πίνακας 1: Βασικοί ρόλοι κόμβων σε δίκτυα blockchain 28
Πίνακας 2: Διαφορές Fog και Edge Computing 56
Πίνακας 3: Ερωτήματα ανά κεφάλαιο 61
Πίνακας 4: Κατανομή από συγκεκριμένους ακαδημαϊκούς εκδότες 68
Πίνακας 5: Κατανομή επιλεγμένων πηγών ανά χρονικές περιόδους..... 69
Πίνακας 6: Κατηγοριοποίηση Επιθέσεων σε Fog και Edge Περιβάλλοντα..... 87
Πίνακας 7: Αντιστοίχιση Τρωτοτήτων Ιδιωτικότητας με Συναφείς Τρωτότητες Ασφάλειας, Επιθέσεις και Παραβιάσεις Ασφάλειας–Ιδιωτικότητας 97
Πίνακας 8: Συνοπτική αποτίμηση οφελών και ευκαιριών του blockchain για την ασφάλεια σε fog/edge περιβάλλοντα 104
Πίνακας 9: Συνοπτική αποτίμηση οφελών και ευκαιριών του blockchain για την ιδιωτικότητα σε fog/edge περιβάλλοντα 109
Πίνακας 10: Αντιστοίχιση προκλήσεων με ερευνητικές κατευθύνσεις σε fog/edge-blockchain.....119

Λίστα Ακρωνύμιων

Ακρωνύμιο	**Πλήρης Όρος**
API	Application Programming Interface
CVE	Common Vulnerabilities and Exposures
DApp	Decentralized Application
DLT	Distributed Ledger Technology
DP	Differential Privacy
GDPR	General Data Protection Regulation
HE	Homomorphic Encryption
IoT	Internet of Things
MEC	Multi-access Edge Computing
ML	Machine Learning
MPC / SMPC	(Secure) Multi-Party Computation
PoA	Proof of Authority
PoS	Proof of Stake
PoW	Proof of Work
RBAC	Role-Based Access Control
SLA	Service Level Agreement
TLS	Transport Layer Security
VPN	Virtual Private Network
ZKP	Zero-Knowledge Proof
zk-SNARK	Zero-Knowledge Succinct Non-Interactive Argument of Knowledge

1. Εισαγωγή

1.1 Τεχνολογίες Blockchain, Fog & Edge Computing

Η εκρηκτική ανάπτυξη του Διαδικτύου των Πραγμάτων (Internet of Things – IoT) και των κατανεμημένων εφαρμογών έχει φέρει στο προσκήνιο πληθώρα τεχνικών και λειτουργικών προκλήσεων. Οι σύγχρονες εφαρμογές απαιτούν συλλογή, ανάλυση και λήψη αποφάσεων σε πραγματικό ή σχεδόν πραγματικό χρόνο, βασιζόμενες σε μεγάλους όγκους δεδομένων που προέρχονται από διαφορετικές γεωγραφικές τοποθεσίες, αισθητήρες και ετερογενείς συσκευές. Το παραδοσιακό, κεντροποιημένο μοντέλο επεξεργασίας δεδομένων όπου όλα τα δεδομένα μεταφέρονται σε ένα απομακρυσμένο υπολογιστικό νέφος (cloud) για αποθήκευση και ισχυρή ανάλυση παρουσιάζει σημαντικά μειονεκτήματα: υψηλή καθυστέρηση, αυξημένο ρίσκο απώλειας δεδομένων, έλλειψη εμπιστοσύνης στους κεντρικούς παρόχους, περιορισμένη δυνατότητα ελέγχου και δυσκολία κλιμάκωσης. Επιπλέον, η εγγύτητα των δεδομένων σε πραγματικές ανθρώπινες δραστηριότητες δημιουργεί ισχυρές απαιτήσεις για ασφάλεια και προστασία ιδιωτικότητας, οι οποίες δύσκολα ικανοποιούνται σε κεντρικά μοντέλα διαχείρισης.

Αυτά τα προβλήματα υποδεικνύουν την ανάγκη για νέες, αποκεντρωμένες αρχιτεκτονικές, οι οποίες θα μπορούν να διαχειρίζονται τοπικά τα δεδομένα – όσο πιο κοντά στο σημείο δημιουργίας τους περιορίζοντας την εξάρτηση από κεντρικά κέντρα επεξεργασίας και ταυτόχρονα προσφέροντας επαρκείς εγγυήσεις και ακεραιότητας, εμπιστευτικότητας διαθεσιμότητας. Σε αυτό το πλαίσιο, τρεις τεχνολογίες έχουν αναδυθεί ως κρίσιμα δομικά στοιχεία: το blockchain, ο ομιχλώδης υπολογισμός (fog computing) και ο υπολογισμός στις ακμές του δικτύου (edge computing). Αν και έχουν σχεδιαστεί με διαφορετικές αφετηρίες και σκοπούς, η συνδυαστική ή συμπληρωματική αξιοποίησή τους υπόσχεται σημαντικά οφέλη για τα σύγχρονα κατανεμημένα περιβάλλοντα και δυνητικά μια ισχυρή αντιμετώπιση των προαναφερόμενων προκλήσεων.

Το blockchain αποτελεί μια τεχνολογία κατανεμημένου καθολικού (distributed ledger), η οποία επιτρέπει την αποθήκευση και επαλήθευση πληροφοριών χωρίς την ανάγκη ύπαρξης εμπιστευόμενου τρίτου μέρους (trusted third-party). Μέσω αλγορίθμων συναίνεσης (consensus algorithms) και κρυπτογραφικών μηχανισμών, διασφαλίζει την ακεραιότητα των δεδομένων, την ανιχνευσιμότητα των συναλλαγών και την αντίσταση σε παραβιάσεις. Οι δυνατότητές του επεκτείνονται με τη χρήση έξυπνων συμβολαίων (smart contracts), τα οποία επιτρέπουν την αυτόματη και αδιαμεσολάβητη εκτέλεση (επιχειρησιακών) κανόνων και πολιτικών. Το blockchain προσφέρει έτσι έναν αξιόπιστο τρόπο διαχείρισης της εμπιστοσύνης, ιδιαίτερα σε περιβάλλοντα με πολλαπλούς συμμετέχοντες και απουσία κοινής αρχής ελέγχου. Οι τεχνικές πτυχές της λειτουργίας του blockchain αναλύονται εκτενώς στο Κεφάλαιο 2

Το fog computing έρχεται να γεφυρώσει το χάσμα μεταξύ του cloud και των τερματικών συσκευών, παρέχοντας υπολογιστική και αποθηκευτική ισχύ σε επίπεδο τοπικών ή περιφερειακών κόμβων. Οι κόμβοι ομίχλης (fog nodes) είναι σε θέση να εκτελούν προκαταρκτική επεξεργασία δεδομένων, να υποστηρίζουν εφαρμογές χαμηλής καθυστέρησης και να επιτρέπουν τον έλεγχο της

τοποθεσίας, των πόρων και των πολιτικών ασφάλειας των δεδομένων και των συσκευών από τους διαχειριστές ή τα αρμόδια συστήματα. Ένα από τα σημαντικότερα πλεονεκτήματά του είναι ότι υποστηρίζει εφαρμογές που απαιτούν συντονισμό μεταξύ πολλών συσκευών σε τοπικό επίπεδο κάτι που το απομακρυσμένο νέφος αδυνατεί να υποστηρίξει αποτελεσματικά. Οι τεχνικές λεπτομέρειες της αρχιτεκτονικής fog computing (επίπεδα, λειτουργίες, μηχανισμοί επεξεργασίας) παρουσιάζονται στο Κεφάλαιο 2.

Το edge computing, από την άλλη πλευρά, πηγαίνει ένα βήμα παραπέρα, φέρνοντας την υπολογιστική ισχύ απευθείας στην "άκρη" του δικτύου δηλαδή στις ίδιες τις συσκευές ή στους αμέσως γειτονικούς πόρους τους. Αυτό μειώνει ακόμα περισσότερο τη χρονική καθυστέρηση και επιτρέπει την άμεση απόκριση χωρίς να απαιτείται ενδιάμεση μετάδοση δεδομένων. Το edge computing ενδείκνυται ιδιαιτέρως για εφαρμογές που χρειάζονται αυστηρούς χρόνους απόκρισης ή λειτουργούν σε περιβάλλοντα με περιορισμένη συνδεσιμότητα. Παράλληλα, μειώνει το εύρος ζώνης που καταναλώνεται για μεταφορές δεδομένων προς το νέφος, πράγμα που υποστηρίζεται και από το fog computing) και περιορίζει την έκθεση των δεδομένων σε τρίτους. Τα τεχνικά χαρακτηριστικά και η πλήρης αρχιτεκτονική του edge computing παρουσιάζονται αναλυτικά στο Κεφάλαιο 2.

Η αξιοποίηση αυτών των τεχνολογιών δεν είναι απαραίτητα ενιαία ή απόλυτα συνδυαστική, καθώς το fog και το edge computing, παρά τη συγγένειά τους, δεν αποτελούν απολύτως συμβατές ή εναλλάξιμες λύσεις. Ωστόσο, ο συνδυασμός του blockchain με το καθένα από αυτά τα δύο υπολογιστικά πρότυπα έχει αποδειχθεί ιδιαίτερα αποτελεσματικός όπως τεκμηριώνεται σε μελέτες που επικεντρώνονται σε fog computing [2] [13] και edge computing [3] [16] [17]. Ειδικότερα, η ενσωμάτωση του blockchain σε περιβάλλοντα fog και edge μπορεί να ενισχύσει τη διαφάνεια, την εμπιστοσύνη και την ανθεκτικότητα, δημιουργώντας ένα ενιαίο, ασφαλές και επεκτάσιμο οικοσύστημα. Η παρούσα εργασία επικεντρώνεται ακριβώς σε αυτή τη συνδυαστική προσέγγιση: πώς οι αρχιτεκτονικές fog και edge μπορούν να επωφεληθούν από την ενσωμάτωση του blockchain για την αντιμετώπιση κρίσιμων ζητημάτων ασφάλειας, ιδιωτικότητας και λειτουργικής αξιοπιστίας στα κατανεμημένα περιβάλλοντα του σήμερα.

Ωστόσο, υπάρχουν σημαντικές προκλήσεις που πρέπει να ληφθούν υπόψιν πριν ο συνδυασμός αυτών των 3 τεχνολογιών ευδοκιμήσει. Πρωτίστως, η ασφάλεια των δεδομένων πριν από την ενσωμάτωσή τους σε ένα κατανεμημένο μητρώο εξαρτάται από το επίπεδο προστασίας που εφαρμόζεται στους κόμβους ομίχλης και ακμής, οι οποίοι, σε σύγκριση με τους αντίστοιχους του υπολογιστικού νέφους, διαθέτουν συνήθως περιορισμένους πόρους και ασθενέστερες δικλείδες ασφαλείας. Επιπλέον, η αυξημένη πολυπλοκότητα στην υλοποίηση κατανεμημένων υποδομών και η ανάγκη συνεχούς συντονισμού μεταξύ πολλών ετερογενών συστημάτων ενδέχεται να επιβαρύνουν τον σχεδιασμό και τη διαχείριση τέτοιων λύσεων.

Παρότι οι θετικές πλευρές περιλαμβάνουν τη χαμηλή καθυστέρηση, την αποκεντρωμένη φύση και την ενίσχυση της προστασίας δεδομένων, οι αρνητικές πλευρές, όπως η αργή επεξεργασία του blockchain, η ευπάθεια των fog και edge κόμβων και η πολυπλοκότητα της διαχείρισης, υπογραμμίζουν την

ανάγκη για περαιτέρω βελτιστοποίηση. Αυτές οι προκλήσεις προετοιμάζουν το έδαφος για τη συνεισφορά της παρούσας εργασίας, η οποία θα αναλυθεί στην επόμενη ενότητα.

1.2 Συνεισφορά της Διπλωματικής Εργασίας

1.2.1 Προσδιορισμός Ερευνητικού Κενού στον Συνδυασμό Blockchain με Fog και Edge Computing

Παρά την αυξανόμενη υιοθέτηση των τεχνολογιών blockchain, fog computing και edge computing σε εφαρμογές του Διαδικτύου των Πραγμάτων (IoT), η σχετική βιβλιογραφία τείνει να τις εξετάζει αποσπασματικά ή σε ζεύγη, αποφεύγοντας μια ενιαία και συστηματική προσέγγιση ως προς τη συνδυαστική τους εφαρμογή. Η έρευνα παραμένει αποσπασματική ως προς το πώς η αποκεντρωμένη ασφάλεια και ακεραιότητα του blockchain μπορεί να ενσωματωθεί σε πολυεπίπεδα κατανεμημένα περιβάλλοντα, όπου η επεξεργασία δεδομένων εκτελείται είτε σε κόμβους fog είτε απευθείας στις συσκευές edge. Ειδικότερα, δεν έχει ακόμα αποτυπωθεί με επάρκεια πώς η τριπλή συνέργεια των εν λόγω τεχνολογιών μπορεί να αξιοποιηθεί για την ενίσχυση της διαφάνειας, της εμπιστευτικότητας και της επιχειρησιακής αποδοτικότητας σε κατανεμημένα συστήματα που απαιτούν χαμηλή καθυστέρηση, τοπική αυτονομία και ισχυρούς μηχανισμούς προστασίας δεδομένων. Η παρούσα εργασία στοχεύει να καλύψει αυτό το κενό, προσφέροντας μια δομημένη ανασκόπηση των υφιστάμενων λύσεων και προσεγγίσεων, αναδεικνύοντας τα σημεία τομής, τις προκλήσεις, αλλά και τις μελλοντικές ερευνητικές διαδρομές που προκύπτουν από τον συνδυασμό αυτών των τριών τεχνολογιών.

1.2.2 Σκοπός και Στόχοι της Έρευνας

Ο σκοπός της εργασίας είναι να παρουσιάσει μια ολοκληρωμένη επισκόπηση των εφαρμογών του blockchain σε περιβάλλοντα fog και edge computing, εστιάζοντας σε υπάρχουσες έρευνες και τις τεχνολογικές προόδους που έχουν γίνει στον τομέα. Η εργασία αναλύει τα πλεονεκτήματα, τις προκλήσεις και τις καινοτόμες προσεγγίσεις που προκύπτουν από τον συνδυασμό αυτών των τριών τεχνολογιών, προσδιορίζοντας τις περιοχές στις οποίες η συνεργασία τους μπορεί να προσφέρει τα μεγαλύτερα οφέλη. Επιπλέον, η εργασία καταγράφει τις κύριες ερευνητικές κατευθύνσεις που έχουν ακολουθηθεί στην επιστημονική βιβλιογραφία, καθώς και τις προοπτικές για μελλοντική έρευνα και ανάπτυξη.

1.2.3 Αναδυόμενες Καινοτομίες & Καινοτόμες Προσεγγίσεις

Αν και η εργασία δεν περιλαμβάνει πρωτογενή έρευνα, η συνεισφορά της βρίσκεται στην συστηματική ανασκόπηση και σύγκριση διαφορετικών μελετών που αναφέρονται στον συνδυασμό των τεχνολογιών blockchain, fog και edge

computing. Μέσω αυτής της επισκόπησης, αναδεικνύεται η καινοτομία που προκύπτει από τις προτάσεις των ερευνητών για την εφαρμογή της τεχνολογίας blockchain σε περιβάλλοντα με περιορισμένους πόρους και υψηλές απαιτήσεις ασφάλειας. Ιδιαίτερη έμφαση δίδεται στις νέες τεχνικές μηχανισμών συναίνεσης και την εφαρμογή των έξυπνων συμβολαίων (smart contracts) για την ασφαλή και αποδοτική διαχείριση των δεδομένων μεταξύ των συσκευών και των κόμβων του δικτύου.

1.2.4 Αναμενόμενα Οφέλη

Η ανασκόπηση της υπάρχουσας βιβλιογραφίας παρέχει πολύτιμα στοιχεία για την κατανόηση των πλεονεκτημάτων και των περιορισμών που σχετίζονται με την ενσωμάτωση του blockchain σε fog και edge computing. Μέσω της σύνθεσης των ευρημάτων, η εργασία προσφέρει καθοδήγηση για μελλοντικές έρευνες και ανάπτυξη εφαρμογών σε τομείς όπως το IoT, οι έξυπνες πόλεις και η αυτόνομη οδήγηση. Επιπλέον, οι στρατηγικές που προτείνονται για την ενίσχυση της ασφάλειας, της διαλειτουργικότητας και της αξιοπιστίας σε κατανεμημένα συστήματα θα μπορούσαν να εφαρμοστούν και να ενισχυθούν από ερευνητές και επαγγελματίες του κλάδου.

1.2.5 Προτάσεις για Μελλοντική Έρευνα

Αν και η υπάρχουσα βιβλιογραφία έχει καλύψει σημαντικές πτυχές του συνδυασμού του blockchain με το fog και το edge computing, υπάρχουν πολλές “προβληματικές” περιοχές καθώς και υποσχόμενες ερευνητικές κατευθύνσεις που χρήζουν περαιτέρω διερεύνησης. Κάποιες από αυτές περιλαμβάνουν τη βελτίωση των μηχανισμών συναίνεσης για την επίλυση προβλημάτων που προκύπτουν από την κατανεμημένη φύση των συστημάτων, την αξιολόγηση της απόδοσης αυτών των συστημάτων σε πραγματικά σενάρια χρήσης, και τη βελτίωση της ενσωμάτωσης του blockchain σε περιβάλλοντα με περιορισμένους πόρους. Επιπλέον, η διερεύνηση των προκλήσεων που σχετίζονται με την κλίμακα, την ενεργειακή αποδοτικότητα και την ασφάλεια των συστημάτων αυτών παραμένει κρίσιμη για την περαιτέρω εξέλιξή τους.

1.3 Δομή της Αναφοράς της Διπλωματικής

Η παρούσα διπλωματική εργασία είναι οργανωμένη σε κεφάλαια, τα οποία ακολουθούν λογική αλληλουχία και καλύπτουν όλες τις πτυχές της χρήσης του blockchain στον υπολογισμό στην ομίχλη (fog computing) και στις άκρες του δικτύου (edge computing). Κάθε κεφάλαιο εξετάζει ένα συγκεκριμένο θέμα που συνεισφέρει στην κατανόηση των τριών αυτών τεχνολογιών και της συνεισφοράς τους στην ασφάλεια, την ιδιωτικότητα και την αποδοτικότητα των κατανεμημένων συστημάτων.

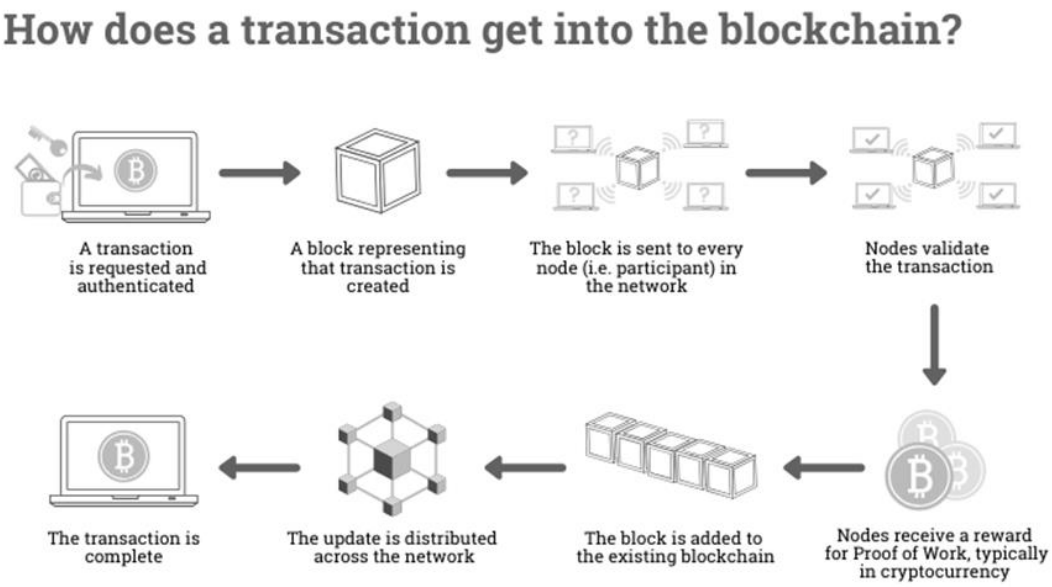
Το πρώτο κεφάλαιο εισάγει το θέμα, τον σκοπό της μελέτης και τα βασικά ερευνητικά ερωτήματα. Το δεύτερο κεφάλαιο παρουσιάζει το θεωρητικό υπόβαθρο για τις 3 τεχνολογίες υπό εστίαση, δηλαδή το blockchain, fog και edge computing. Το τρίτο κεφάλαιο περιγράφει τη μεθοδολογία βιβλιογραφικής

ανασκόπησης που εφαρμόστηκε. Το τέταρτο κεφάλαιο αναλύει ζητήματα ασφάλειας και ιδιωτικότητας στο fog και edge computing καθώς και σχετικές προκλήσεις αλλά και λύσεις που είναι ανεξάρτητες από το blockchain. Το πέμπτο κεφάλαιο εξετάζει τη συμβολή του blockchain στην αντιμετώπιση ζητημάτων ασφάλειας και ιδιωτικότητας στο fog και edge computing. Το έκτο κεφάλαιο εστιάζει στις προκλήσεις και τις ερευνητικές κατευθύνσεις που σχετίζονται με την εφαρμογή του blockchain σε fog και edge περιβάλλοντα, δίνοντας ιδιαίτερη έμφαση σε ζητήματα απόδοσης, κατανάλωσης πόρων, ασφάλειας και ιδιωτικότητας αλλά και στη χρήση τεχνολογιών αιχμής. Τέλος, το όγδοο κεφάλαιο παρουσιάζει τα συνολικά συμπεράσματα της εργασίας, αποτιμά τη συνεισφορά και τα οφέλη της διπλωματικής, συνοψίζει τα βασικά ευρήματα και διατυπώνει τελικές ερευνητικές προοπτικές.

2. Υπόβαθρο

Η τεχνολογική καινοτομία αποτελεί τη βάση για τις εξελίξεις στον ψηφιακό κόσμο. Το κεφάλαιο αυτό εξετάζει τρεις βασικές τεχνολογίες που συμβάλλουν στη δημιουργία αποκεντρωμένων, ασφαλών και αποδοτικών συστημάτων: το blockchain, το fog computing και το edge computing. Παρουσιάζονται τα θεμελιώδη στοιχεία κάθε τεχνολογίας, η αρχιτεκτονική τους, καθώς και οι εφαρμογές τους. Παράλληλα, αναλύονται τα πλεονεκτήματα και οι περιορισμοί τους, προετοιμάζοντας το έδαφος για τη συνδυαστική χρήση τους σε καινοτόμες λύσεις. Η ανάλυση των τριών αυτών τεχνολογιών πραγματοποιείται στις τρεις βασικές ενότητες του τρέχοντος κεφαλαίου, αντίστοιχα.

2.1 Blockchain



Εικόνα 1: Απεικόνιση επικύρωσης μια συναλλαγής σε μια αλυσίδα blockchain [12].

Η ενότητα αυτή εισάγει την τεχνολογία blockchain, παρουσιάζοντας τον ορισμό της και τα βασικά στοιχεία που τη διακρίνουν, θέτοντας το πλαίσιο για τις επόμενες υποενότητες που αναλύουν τη λειτουργία, την αρχιτεκτονική και τις εφαρμογές της.

2.1.1 Ορισμοί Βασικών Εννοιών του Blockchain

Το blockchain είναι απλώς μια αλυσίδα από blocks δεδομένων, επικυρωμένα από ένα δίκτυο κόμβων, όπου κάθε μπλοκ έχει σημείο αναφοράς στο προηγούμενο block μέσω μιας κρυπτογραφικής υπογραφής κατακερματισμού, γνωστής ως hash (κατακερματισμός). Ειδικότερα, κάθε block περιέχει ένα hash (ψηφιακό αποτύπωμα των δεδομένων της κεφαλίδας του block) καθώς και το hash του προηγούμενου block. Αυτή η διαδικασία επαναλαμβάνεται διαρκώς

κατά την εισαγωγή νέων μπλοκ, δημιουργώντας μια αλυσίδα από hashes που εκτείνεται έως το πρώτο block, γνωστό ως genesis block (μπλοκ γένεσης). Αυτό διασφαλίζει μια αδιάσπαστη αλυσίδα καταγραφών [4] [6].

Οποιαδήποτε αλλαγή σε ένα block σπάει αυτή την αλυσίδα, καθώς η αλλαγή σε ένα block σημαίνει ότι πρέπει να υπολογιστούν εκ νέου όλα τα hashes των μπλοκ που ακολουθούν. Συνεπώς, ένα βασικό χαρακτηριστικό του blockchain είναι η αμεταβλητότητα (Immutability). Όπως σημειώνει ο Pilkington [4], όταν τα δεδομένα εισάγονται στο blockchain, δεν μπορούν να αφαιρεθούν και παραμένουν εκεί για πάντα. Αυτή η αμεταβλητότητα είναι αποτέλεσμα της ίδιας της δομής του blockchain. Παρόλο που τα δεδομένα κυκλοφορούν σχετικά ελεύθερα στο blockchain, οποιαδήποτε αλλαγή ή διαγραφή δεδομένων από ένα συγκεκριμένο block ή η προσθήκη νέου block σε ενδιάμεσο σημείο διακόπτει την κρυπτογραφική αλυσίδα που συνδέει τα blocks. Στην πράξη, αυτό σημαίνει ότι, μόλις εισαχθούν τα δεδομένα, δεν μπορούν να τροποποιηθούν χωρίς να αλλοιωθεί η ακεραιότητα της αλυσίδας. Στην πράξη, η τροποποίηση ή διαγραφή καταχωρήσεων χωρίς να αλλοιωθεί η ακεραιότητα της αλυσίδας είναι εξαιρετικά δύσκολη, γεγονός που καθιστά το blockchain ασφαλή μηχανισμό καταγραφής δεδομένων ή/και μεταδεδομένων σε κατανεμημένα περιβάλλοντα [2], [4]. Έτσι, το blockchain μετατρέπεται σε έναν ιδιαίτερα ασφαλή μηχανισμό καταγραφής δεδομένων ή μετα-δεδομένων [2].

Ένα από τα βασικά δομικά στοιχεία του οικοσυστήματος blockchain είναι τα έξυπνα συμβόλαια (smart contracts). Τα έξυπνα συμβόλαια είναι αυτοεκτελούμενα προγράμματα με προσυμφωνημένους όρους γραμμένους σε κώδικα. Όταν πληρούνται συγκεκριμένες συνθήκες, ο κώδικας ενεργοποιείται και εκτελεί αυτόματα τη συμφωνία, χωρίς την ανάγκη μεσάζοντα. Αυτά τα συμβόλαια αποθηκεύονται εντός του blockchain, το οποίο διασφαλίζει την ακεραιότητα του περιεχομένου τους, καθώς και την αμεταβλητότητα της λογικής που διέπει την εκτέλεσή τους. Παράλληλα, η ίδια η εκτέλεση του συμβολαίου συχνά συνοδεύεται από την καταγραφή σχετικών δοσοληψιών στο blockchain, παρέχοντας πλήρη διαφάνεια και ιχνηλασιμότητα.

Σε αυτό το πλαίσιο εντάσσονται και οι αποκεντρωμένες εφαρμογές (DApps – Decentralized Applications), οι οποίες χρησιμοποιούν έξυπνα συμβόλαια ως θεμέλιο λειτουργίας. Οι DApps αναπτύσσονται πάνω σε blockchain πλατφόρμες (όπως το Ethereum) και, αντί να εξαρτώνται από κεντρικούς εξυπηρετητές, βασίζονται σε κατανεμημένους κόμβους για την εκτέλεση των λειτουργιών τους. Αυτό σημαίνει ότι ούτε ο κώδικας ούτε τα δεδομένα μπορούν να αλλοιωθούν ή να ελεγχθούν μονομερώς από κάποιον πάροχο ή οργανισμό. Ως αποτέλεσμα, οι DApps χαρακτηρίζονται από αυξημένη ασφάλεια, ανθεκτικότητα σε επιθέσεις και ενισχυμένη διαφάνεια, καθώς η συμπεριφορά τους καθορίζεται από κώδικα που είναι γνωστός και προσβάσιμος στους συμμετέχοντες.

Τα δεδομένα που αποθηκεύονται στο blockchain συνήθως δεν περιλαμβάνουν τις πλήρεις λεπτομέρειες κάθε συναλλαγής, παρά μόνο μεταδεδομένα (metadata) για αυτές και ειδικότερα τις πληροφορίες που είναι αναγκαίες για την επαλήθευση και επιβεβαίωση της συναλλαγής. Τα μεταδεδομένα αυτά περιλαμβάνουν πληροφορίες σχετικές με μια συναλλαγή (metadata), όπως χρονικές σφραγίδες και συνοπτικά στοιχεία, χωρίς να αποκαλύπτουν

ευαίσθητα στοιχεία. Αυτή η προσέγγιση εξασφαλίζει την αποδοτικότητα της αποθήκευσης, διατηρώντας ταυτόχρονα την ακεραιότητα και ιδιωτικότητα των δεδομένων.

Η προσθήκη νέων blocks (όπου κάθε μπλοκ περιλαμβάνει μια σειρά από δεδομένα συναλλαγών) γίνεται μέσω μηχανισμών συναίνεσης, όπως τον proof-of-work (PoW) ή τον proof-of-stake (PoS). Αυτοί οι αλγόριθμοι διασφαλίζουν ότι όλοι οι κόμβοι του δικτύου συμφωνούν σχετικά με την εγκυρότητα ενός block πριν προστεθεί στην αλυσίδα. Έτσι, το blockchain παραμένει αποκεντρωμένο και ανθεκτικό σε κακόβουλες ενέργειες.

Οι κόμβοι (nodes) στο blockchain είναι υπολογιστικές μονάδες που διατηρούν ένα πλήρες αντίγραφο της αλυσίδας και συμμετέχουν στη διαδικασία συναίνεσης. Όλοι οι κόμβοι είναι απαραίτητοι για τη διατήρηση της ακεραιότητας του δικτύου και την αποφυγή καταστάσεων ή ζητημάτων ασφαλείας, όπως οι διπλές δαπάνες (double spending).

Το blockchain δεν είναι μόνο ένα εργαλείο αποθήκευσης δεδομένων. Επιτρέπει τη δημιουργία έξυπνων συμβολαίων (smart contracts), τα οποία είναι αυτοματοποιημένοι κανόνες που εκτελούνται όταν πληρούνται συγκεκριμένες συνθήκες. Αυτή η δυνατότητα επεκτείνει τη χρήση του blockchain σε τομείς, όπως η διαχείριση της εφοδιαστικής αλυσίδας, οι ψηφιακές ταυτότητες και οι ασφαλείς συναλλαγές.

Ο συνδυασμός αυτών των ιδιοτήτων καθιστά το blockchain όχι απλώς μια υποδομή αποθήκευσης δεδομένων, αλλά ένα θεμέλιο για τη δημιουργία αποκεντρωμένων, αυτόνομων και ασφαλών ψηφιακών οικοσυστημάτων, εντός των οποίων κάθε ενέργεια είναι ανιχνεύσιμη, κάθε συμβόλαιο εκτελείται όπως έχει προγραμματιστεί και κάθε εφαρμογή λειτουργεί χωρίς σημείο αποτυχίας ή εξάρτησης από ενδιάμεσους φορείς [2] [4].

2.1.2 Είδη Blockchain

Το blockchain μπορεί να ταξινομηθεί σε τέσσερις βασικούς τύπους ανάλογα με τη χρήση και την αρχιτεκτονική του: δημόσιο (public), ιδιωτικό (private), συνεργατικό (consortium) και υβριδικό (hybrid).

Το δημόσιο blockchain είναι πλήρως αποκεντρωμένο και ανοιχτό σε οποιονδήποτε. Κάθε χρήστης μπορεί να συμμετέχει ως κόμβος και άρα να επαληθεύει συναλλαγές ή/και να δημιουργεί blocks. Το δημόσιο blockchain χρησιμοποιεί μηχανισμούς συναίνεσης, όπως το Proof-of-Work (PoW) ή το Proof-of-Stake (PoS), εξασφαλίζοντας τη διαφάνεια και την ασφάλεια του δικτύου. Ενδεικτικά παραδείγματα δημοσίων blockchain αποτελούν τα Bitcoin[1] [1] και Ethereum[2] [21]. Αν και προσφέρει υψηλό επίπεδο εμπιστοσύνης χωρίς την ανάγκη κεντρικού διαμεσολαβητή, το δημόσιο blockchain έχει σημαντικά

[1] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[2] V. Buterin, *A Next-Generation Smart Contract and Decentralized Application Platform*, Ethereum White Paper, 2014. [Online]. Available: https://ethereum.org/en/whitepaper/

μειονεκτήματα, όπως υψηλή κατανάλωση ενέργειας (ιδίως με PoW) και χαμηλότερη ταχύτητα συναλλαγών σε σύγκριση με άλλα είδη blockchain [8] [9].

Το ιδιωτικό blockchain λειτουργεί εντός ενός περιορισμένου δικτύου και επιτρέπει τη συμμετοχή μόνο σε εξουσιοδοτημένους χρήστες. Χρησιμοποιείται συνήθως από οργανισμούς για εσωτερική διαχείριση δεδομένων, αλλά και σε εμπορικές εφαρμογές, όπως συστήματα εφοδιαστικής αλυσίδας, καθώς και σε διατραπεζικές συναλλαγές, όπως οι πληρωμές μεταξύ διαφορετικών τραπεζών (cross-border transactions). Χαρακτηριστικά παραδείγματα ιδιωτικών blockchain είναι τα Hyperledger[3] [22] και Corda[4] [23]. Τα πλεονεκτήματά ενός ιδιωτικού blockchain περιλαμβάνουν ταχύτερη επεξεργασία συναλλαγών λόγω περιορισμένου αριθμού κόμβων, καθώς και μεγαλύτερο έλεγχο στη διαχείριση της πρόσβασης. Επιπλέον, προσφέρει μεγαλύτερη κλιμακωσιμότητα και ευέλικτη διοίκηση. Η κλιμακωσιμότητα επιτυγχάνεται λόγω του περιορισμένου αριθμού κόμβων, με αποτέλεσμα τη ταχύτερη επεξεργασία συναλλαγών και τη καλύτερη απόδοση σε μεγαλύτερης κλίμακας δίκτυα. Ενώ, η ευέλικτη διοίκηση επιτρέπει στους οργανισμούς να προσαρμόζουν τους κανόνες και τα πρωτόκολλα του δικτύου σύμφωνα με τις ειδικές ανάγκες τους, παρέχοντας έτσι μεγαλύτερο έλεγχο στη διαχείριση των δεδομένων και της πρόσβασης. Παρόλα αυτά, ένα ιδιωτικό blockchain μειονεκτεί σε σχέση με τη διαφάνεια που παρέχουν τα δημόσια και συχνά εξαρτάται και ελέγχεται από έναν κεντρικό φορέα [8] [9].

Το συνεργατικό/κοινοτικό blockchain (consortium blockchain) αποτελεί μια υβριδική μορφή που συνδυάζει χαρακτηριστικά από δημόσια και ιδιωτικά blockchain. Διοικείται από μια ομάδα οργανισμών και προσφέρει ευελιξία στη διαχείριση δεδομένων και την πρόσβαση. Παραδείγματα συνεργατικών blockchain είναι τα Quorum[5] [24] και Ripple[6] [25]. Το συνεργατικό blockchain παρέχει ισορροπία μεταξύ αποκέντρωσης και διακυβέρνησης, ενώ διατηρεί μέτρια κλιμακωσιμότητα και επεκτασιμότητα, καθώς συμμετέχουν σε αυτό περισσότεροι κόμβοι από ένα ιδιωτικό δίκτυο αλλά λιγότεροι από ένα δημόσιο. Η συμμετοχή πολλών οργανισμών συνεπάγεται πολιτικές συνδιαχείρισης, που μπορεί να επιβαρύνουν τη λήψη αποφάσεων ή την ευελιξία στην υλοποίηση αλλαγών, καθώς απαιτείται συναίνεση από διαφορετικά μέρη [10]. Εφαρμογές συνεργατικού blockchain εμφανίζονται σε συστήματα κοινής εφοδιαστικής αλυσίδας (multi-company supply chains), αλλά και σε σενάρια διατραπεζικής συνεργασίας, όπως οι cross-border payments μεταξύ τραπεζών.

Το Υβριδικό Blockchain (Hybrid Blockchain) συνδυάζει τα χαρακτηριστικά του δημόσιου και του ιδιωτικού blockchain. Ορισμένες λειτουργίες και δεδομένα είναι δημόσια προσβάσιμα, ενώ άλλα παραμένουν ιδιωτικά, προσφέροντας ισχυρή ευελιξία στη διαχείριση πρόσβασης και ασφάλειας. Αυτή η προσέγγιση επιτρέπει την αποτελεσματική προστασία ευαίσθητων δεδομένων, παράλληλα με τη διατήρηση της δυνατότητας δημόσιας επικύρωσης (auditability) σε κρίσιμες λειτουργίες. Χρήση υβριδικών μοντέλων έχει παρατηρηθεί σε

[3] Hyperledger Foundation, *Hyperledger Fabric Documentation*, [Online]. Available: https://hyperledger-fabric.readthedocs.io/
[4] R3, *Corda Platform Overview*, [Online]. Available: https://www.r3.com/corda-platform/
[5] ConsenSys, *Quorum Blockchain Platform*, [Online]. Available: https://consensys.net/quorum/
[6] Ripple, *RippleNet Overview*, [Online]. Available: https://ripple.com/ripplenet/

εμπορικές εφαρμογές όπου απαιτείται ελεγχόμενη διαφάνεια, καθώς και στη διαχείριση ιατρικών δεδομένων, όπου η προστασία της ιδιωτικότητας συνδυάζεται με την επικύρωση των καταγραφών από εξωτερικούς φορείς. Ενδεικτικά παραδείγματα αποτελούν το Dragonchain[7] [26] και το IBM Blockchain[8] [27]. Αν και το υβριδικό μοντέλο συνδυάζει τα πλεονεκτήματα των άλλων τύπων, είναι πιο περίπλοκο στην υλοποίηση και απαιτεί αυξημένες απαιτήσεις σε υποδομή και διαχείριση, γεγονός που συνεπάγεται συνεχή παρακολούθηση για την ομαλή λειτουργία.

Οι τέσσερις αυτοί τύποι blockchain καλύπτουν διαφορετικές ανάγκες και προσφέρουν μοναδικές δυνατότητες, ανάλογα με τις απαιτήσεις της εφαρμογής ή του οργανισμού που τα χρησιμοποιεί.

2.1.3 Χαρακτηριστικά & Οφέλη του Blockchain

Το blockchain αποτελεί μια αποκεντρωμένη υποδομή κατανεμημένου μητρώου που εγγυάται την ασφάλεια, τη διαφάνεια, τη διαθεσιμότητα και την αμεταβλητότητα των δεδομένων, αξιοποιώντας μηχανισμούς κρυπτογράφησης και συναίνεσης. Η συγκεκριμένη ενότητα αναλύει τα βασικά λειτουργικά και αρχιτεκτονικά χαρακτηριστικά του blockchain, εστιάζοντας σε εκείνα που σχετίζονται άμεσα με την αξιοπιστία, την εμπιστευτικότητα, και την αποτελεσματικότητα του συστήματος που υιοθετεί το blockchain.

Αποκέντρωση και Κατανεμημένη Αρχιτεκτονική

Σε αντίθεση με τις κλασικές συγκεντρωτικές βάσεις δεδομένων, το blockchain βασίζεται σε μια αρχιτεκτονική peer-to-peer (P2P), όπου το μητρώο (των δεδομένων/συναλλαγών) αντιγράφεται και συντηρείται ταυτόχρονα από μεγάλο αριθμό συμμετεχόντων κόμβων. Η διαχείριση είναι διαμοιρασμένη και οι αλλαγές στα δεδομένα απαιτούν τη συναίνεση του δικτύου, μειώνοντας τα κεντρικά σημεία αστοχίας και καθιστώντας το σύστημα πιο ανθεκτικό σε επιθέσεις ή σφάλματα [4]. Σημειώνεται ωστόσο ότι σε ιδιωτικά ή συνεργατικά blockchain, μπορεί να υφίσταται περιορισμένη κεντρική διαχείριση.

Επικύρωση Χωρίς Εμπιστοσύνη (Trustless Verification)

Το blockchain καθιστά περιττή την παρουσία ενδιάμεσων εμπιστευτικών φορέων για την επιβεβαίωση των δεδομένων/μπλοκ. Οι χρήστες δεν χρειάζεται να εμπιστεύονται κάποιον πάροχο ή οργανισμό: η εγκυρότητα των συναλλαγών προκύπτει από την αποδοχή τους μέσω συμφωνημένων μηχανισμών συναίνεσης. Αυτή η ιδιότητα ενισχύει την αξιοπιστία και την ανθεκτικότητα των κατανεμημένων συστημάτων, επιτρέποντας τη δημιουργία εφαρμογών χωρίς μεσάζοντες [4].

Αμεταβλητότητα και Ακεραιότητα Δεδομένων

[7] Dragonchain, *Dragonchain Overview*, [Online]. Available: https://dragonchain.com/
[8] IBM, *IBM Blockchain Platform*, [Online]. Available: https://www.ibm.com/blockchain/platform

Κάθε block στο blockchain περιλαμβάνει το δικό του μοναδικό hash καθώς και το hash του προηγούμενου block, διαμορφώνοντας μια αλυσίδα αλληλεξαρτώμενων εγγραφών. Η δομή αυτή εξασφαλίζει ότι οποιαδήποτε τροποποίηση των δεδομένων σε ένα block απαιτεί τον ανασχεδιασμό όλων των επόμενων hashes, καθιστώντας πρακτικά αδύνατη την τροποποίηση της αλυσίδας χωρίς να εντοπιστεί η παρέμβαση. Η αμεταβλητότητα αυτή εγγυάται την ακεραιότητα της ιστορικής πληροφορίας [4].

Κρυπτογραφική Ασφάλεια και Μηχανισμοί Συναίνεσης

Η ασφάλεια των δεδομένων ενισχύεται μέσω ισχυρών κρυπτογραφικών τεχνικών, όπως οι ψηφιακές υπογραφές και οι κατακερματισμοί (hash functions), που διασφαλίζουν την ακεραιότητα, την εμπιστευτικότητα και την αμεταβλητότητα των συναλλαγών. Παράλληλα, η εγκυρότητα και η προσθήκη νέων blocks στην αλυσίδα εξασφαλίζονται μέσω αλγορίθμων συναίνεσης. Οι δύο επικρατέστεροι είναι το Proof of Work (PoW) και το Proof of Stake (PoS). Στο PoW, οι εξορυκτές (miners) λύνουν δύσκολα υπολογιστικά παζλ για την επαλήθευση συναλλαγών, κάτι που προσφέρει υψηλό επίπεδο ασφάλειας αλλά συνεπάγεται υψηλή ενεργειακή κατανάλωση. Αντίθετα, το PoS βασίζεται στην ποσότητα tokens που "στοιχηματίζει" κάθε κόμβος, αποφεύγοντας το ενεργειακό κόστος, αλλά εισάγοντας πιθανότητες οικονομικού συγκεντρωτισμού [4].

Διαφάνεια και Ανιχνευσιμότητα

Ένα από τα σημαντικότερα πλεονεκτήματα του blockchain είναι η διαφάνεια που προσφέρει. Κάθε συμμετέχων έχει τη δυνατότητα να επαληθεύσει οποιαδήποτε συναλλαγή. Οι συναλλαγές καταγράφονται σε blocks τα οποία αναπαράγονται σε όλο το δίκτυο, καθιστώντας τις τροποποιήσεις πρακτικά αδύνατες χωρίς συναίνεση. Η διαφάνεια αυτή είναι καθοριστική σε τομείς, όπως οι χρηματοοικονομικές υπηρεσίες, η υγειονομική περίθαλψη και η εφοδιαστική αλυσίδα, όπου απαιτείται τεκμηριωμένη λογοδοσία [2].

Αξιοπιστία και Ανθεκτικότητα

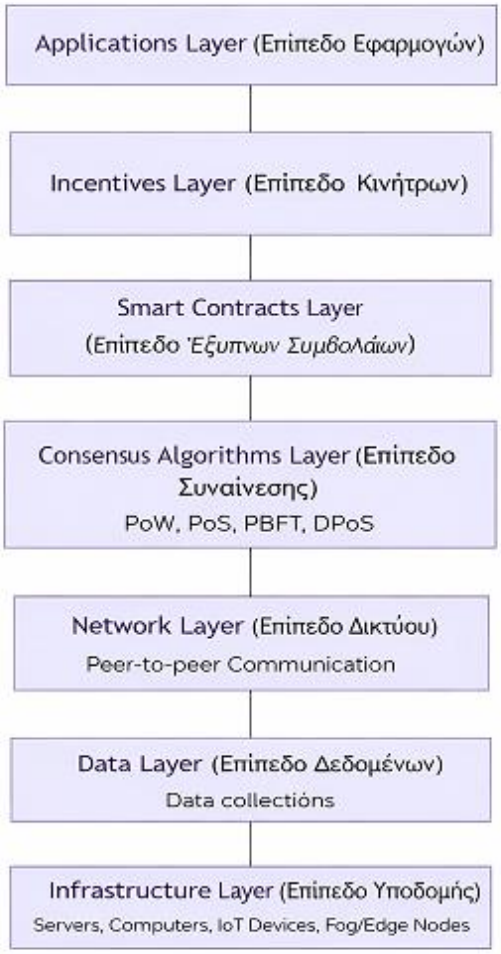
Η λειτουργία του blockchain συνεχίζεται απρόσκοπτα ακόμη και σε περίπτωση αποτυχίας μεμονωμένων κόμβων, χάρη στην ύπαρξη πλεονάζοντων αντιγράφων του μητρώου. Σε περιπτώσεις τεχνικών προβλημάτων ή επιθέσεων, η συγχρονισμένη αποθήκευση εγγυάται την αποκατάσταση των δεδομένων, προσδίδοντας αξιοπιστία και λειτουργική συνέχεια και άρα ανθεκτικότητα [4].

Κρυπτογραφικά Συνδεδεμένα Blocks και Audit Trails

Κάθε block περιλαμβάνει χρονική σήμανση, καταχωρήσεις συναλλαγών και το hash του προηγούμενου block, συγκροτώντας ένα audit trail (μονοπάτι ελέγχου) ενσωματωμένο στη δομή του blockchain. Σε αντίθεση με τα παραδοσιακά audit logs που είναι εξωτερικές αναφορές, τα blocks αποτελούν εγγενείς μονάδες τεκμηρίωσης εντός της ίδιας της αλυσίδας, με ανώτερη ασφάλεια και μη τροποποιήσιμη δομή [4].

2.1.4 Αρχιτεκτονική Blockchain

Η αρχιτεκτονική αποτελεί τη βαση για την εκτέλεση αξιόπιστων, ασφαλών, αποκεντρωμένων και διαφανών συναλλαγών για την κάλυψη ποικιλίας αναγκών. Η αρχιτεκτονική της τεχνολογίας blockchain είναι ένα πολυεπίπεδο σύστημα, που συνδέει διαφορετικά επίπεδα και στοιχεία, εξασφαλίζοντας τη λειτουργικότητα, την ανθεκτικότητα και αξιοπιστία του συστήματος. Η δομή αυτή διασφαλίζει ότι οι συναλλαγές πραγματοποιούνται χωρίς κενά ή ατέλειες, προσφέροντας ανθεκτικότητα και επεκτασιμότητα για πληθώρα εφαρμογών [5].



Εικόνα 2: Η αρχιτεκτονική του Blockchain [5]

Η αρχιτεκτονική του blockchain μπορεί να περιγραφεί με μια ιεραρχική δομή επιπέδων, η οποία αναλύεται στη συνέχεια.

2.1.4.1 Επίπεδο Υποδομής (Infrastructure Layer)

Το επίπεδο υποδομής περιλαμβάνει τους φυσικούς και εικονικούς πόρους πάνω στους οποίους στηρίζεται το blockchain, όπως servers, υπολογιστές, συσκευές IoT, κόμβους fog/edge. Παρέχει τη βασική υπολογιστική και αποθηκευτική ισχύ για την εκτέλεση των ανώτερων επιπέδων και τη διασφάλιση της ακεραιότητας, ασφάλειας και διαθεσιμότητας του δικτύου.

2.1.4.2 Επίπεδο Δεδομένων (Data Layer)

Το επίπεδο δεδομένων καθορίζει τον τρόπο με τον οποίο οργανώνονται, αποθηκεύονται και επαληθεύονται οι πληροφορίες στο blockchain. Κάθε block περιλαμβάνει μεταδεδομένα, το hash του προηγούμενου block και ένα σύνολο συναλλαγών, δημιουργώντας μια αλληλουχία blocks που προσδίδει αμεταβλητότητα και ισχυρή κρυπτογραφική σύνδεση στην αλυσίδα [5].

Η ακεραιότητα των δεδομένων ενισχύεται μέσω δομών όπως τα Merkle Trees, τα οποία επιτρέπουν στους κόμβους να επαληθεύσουν την εγκυρότητα των συναλλαγών με αποδοτικό τρόπο, ακόμα και χωρίς να διαθέτουν ολόκληρο το σύνολο των δεδομένων. Παράλληλα, χρησιμοποιούνται ψηφιακές υπογραφές για την πιστοποίηση των συναλλαγών και την εξασφάλιση ότι οι εντολές προέρχονται από νόμιμους χρήστες του συστήματος.

Το επίπεδο δεδομένων διαχειρίζεται επίσης την αποθήκευση του block header, των hashes και των συναλλαγών, ώστε οποιαδήποτε προσπάθεια τροποποίησης να μπορεί να εντοπιστεί άμεσα λόγω της κρυπτογραφικής ασυνέπειας που θα προκύψει. Η κρυπτογραφική σύνδεση μεταξύ των blocks διασφαλίζει ότι η αλυσίδα δεν μπορεί να αλλοιωθεί χωρίς τον επαναϋπολογισμό όλων των επόμενων blocks, κάτι που είναι υπολογιστικά ανέφικτο σε αποκεντρωμένα περιβάλλοντα [5].

2.1.4.3 Επίπεδο Δικτύου (Network Layer)

Το επίπεδο δικτύου αποτελεί τη θεμελιώδη υποδομή πάνω στην οποία λειτουργεί ολόκληρο το blockchain, καθώς διαχειρίζεται τον τρόπο με τον οποίο οι κόμβοι επικοινωνούν, συγχρονίζονται και ανταλλάσσουν δεδομένα στο πλαίσιο ενός αποκεντρωμένου peer-to-peer (ομότιμου) συστήματος [5]. Αποτελεί την απαραίτητη βάση για την ομαλή λειτουργία των ανώτερων επιπέδων, εξασφαλίζοντας ότι όλες οι συναλλαγές και τα blocks μεταδίδονται με συνέπεια και ασφάλεια.

Οι κόμβοι επικοινωνούν μεταξύ τους ισότιμα, χωρίς κεντρικούς διαμεσολαβητές, γεγονός που προσφέρει ανθεκτικότητα σε επιθέσεις και υψηλή διαθεσιμότητα. Το επίπεδο δικτύου αναλαμβάνει τη διανομή νέων συναλλαγών και blocks, τον συγχρονισμό της κατάστασης όλου του συστήματος, καθώς και την αποστολή σημάτων συμμετοχής στους μηχανισμούς συναίνεσης. Η επικοινωνία και μετάδοση γίνονται μέσω

κρυπτογραφημένων καναλιών, ώστε να προστατεύεται η ακεραιότητα και η ιδιωτικότητα των δεδομένων εντός του κατανεμημένου περιβάλλοντος [5].

Επιπλέον, το επίπεδο δικτύου περιλαμβάνει μηχανισμούς αντιμετώπισης κακόβουλων ενεργειών, όπως απόρριψη μη έγκυρων μηνυμάτων, φιλτράρισμα ύποπτων συνδέσεων και τεχνικές ανωνυμοποίησης για την προστασία της ταυτότητας των κόμβων. Η αποκεντρωμένη αρχιτεκτονική του επιτρέπει στο σύστημα να παραμένει λειτουργικό ακόμη και αν ορισμένοι κόμβοι τεθούν εκτός λειτουργίας, ενώ ο συνεχής συγχρονισμός των δεδομένων διασφαλίζει την ομοιομορφία της πληροφορίας σε όλο το δίκτυο. Χωρίς αυτό το επίπεδο, η λειτουργία της συναίνεσης, η αποθήκευση δεδομένων και η συνολική ακεραιότητα της αλυσίδας δεν θα ήταν εφικτές.

2.1.4.4 Επίπεδο Αλγορίθμων Συναίνεσης (Consensus Algorithms Layer)

Το επίπεδο συναίνεσης είναι υπεύθυνο για την επίτευξη συμφωνίας μεταξύ των κόμβων σχετικά με την εγκυρότητα των συναλλαγών και την κατάσταση του μητρώου. Αποτελεί τον μηχανισμό που επιτρέπει τη λειτουργία του blockchain χωρίς την ύπαρξη κεντρικής αρχής, καθώς προσφέρει έναν τρόπο επαλήθευσης που βασίζεται σε κρυπτογραφικά και υπολογιστικά κριτήρια [5].

Μηχανισμοί όπως οι Proof of Work (PoW) & Proof of Stake (PoS) εξασφαλίζουν ότι τα blocks προστίθενται στην αλυσίδα μετά από διαδικασία επικύρωσης που προστατεύει από επιθέσεις αλλοίωσης ή διπλής δαπάνης. Υπάρχουν επίσης πιο εξελιγμένοι μηχανισμοί όπως το Delegated Proof of Stake (DPoS) και το Practical Byzantine Fault Tolerance (PBFT), που στοχεύουν σε μεγαλύτερη κλιμάκωση ή ταχύτερη συναίνεση. Στο DPoS, οι συμμετέχοντες ψηφίζουν για έναν περιορισμένο αριθμό αντιπροσώπων που αναλαμβάνουν την επικύρωση των blocks, εξασφαλίζοντας μεγαλύτερη ταχύτητα και κλιμάκωση, ενώ διατηρείται η έμμεση συμμετοχή όλων των κόμβων μέσω της ψηφοφορίας. Το PBFT είναι κατάλληλο για μικρότερα ή consortium blockchain και επιτρέπει στο δίκτυο να επιτυγχάνει συναίνεση ακόμα και όταν κάποιοι κόμβοι συμπεριφέρονται κακόβουλα (Byzantine faults), προσφέροντας υψηλή αξιοπιστία και ανθεκτικότητα χωρίς την ανάγκη ενεργειακά απαιτητικών διαδικασιών όπως το PoW.

Το επίπεδο συναίνεσης καθορίζει ποια blocks προστίθενται στην αλυσίδα, ποια απορρίπτονται ως μη έγκυρα και με ποιον τρόπο διασφαλίζεται ότι όλοι οι κόμβοι έχουν την ίδια εικόνα του μητρώου. Η ασφάλεια του blockchain στηρίζεται σε αυτό το επίπεδο, καθώς η αναδρομική αλλοίωση δεδομένων καθίσταται εξαιρετικά δαπανηρή ή υπολογιστικά ανέφικτη λόγω των ενσωματωμένων μηχανισμών συναίνεσης [5].

2.1.4.5 Επίπεδο Έξυπνα Συμβολαίων (Smart Contracts Layer)

Το επίπεδο έξυπνων συμβολαίων αποτελεί το σημείο στο οποίο υλοποιούνται αυτοματοποιημένοι κώδικες που εκτελούνται εντός του blockchain χωρίς τη μεσολάβηση κεντρικής οντότητας. Τα έξυπνα συμβόλαια αποτελούν λογικές εντολές που εκτελούνται όταν πληρούνται συγκεκριμένες προϋποθέσεις,

καθιστώντας δυνατή τη δημιουργία αυτοματοποιημένων και πλήρως διαφανών διαδικασιών [5].

Στο επίπεδο αυτό καταγράφονται όλοι οι κανόνες και οι παράμετροι που καθορίζουν τη λειτουργία μιας διαδικασίας ή μιας συμφωνίας, ενώ η εκτέλεση των έξυπνων συμβολαίων πραγματοποιείται μέσα από ένα καθορισμένο περιβάλλον εκτέλεσης (π.χ. εικονική μηχανή όπως η EVM στο Ethereum). Η εκτέλεση κάθε εντολής συνοδεύεται από υπολογισμό κόστους (gas/fees), ώστε να περιορίζεται η κατανάλωση πόρων του δικτύου και να αποτρέπονται κακόβουλα ή άπειρα loops. Παράλληλα, εφαρμόζονται κανόνες μετάβασης καταστάσεων (state transition rules), οι οποίοι ορίζουν πώς ενημερώνεται η παγκόσμια κατάσταση του blockchain (π.χ. υπόλοιπα λογαριασμών, μεταβλητές συμβολαίων, αποθηκευμένα δεδομένα) μετά από κάθε έγκυρη συναλλαγή ή κλήση συμβολαίου.

Τα έξυπνα συμβόλαια υποστηρίζουν την αυτοματοποίηση λειτουργιών όπως πληρωμές, διαχείριση αποθεμάτων, εφοδιαστική αλυσίδα, εκτέλεση συναλλαγών ή πολύπλοκων μορφών επιχειρησιακής λογικής. Χάρη στην ακεραιότητα και την αμεταβλητότητα του blockchain, τα έξυπνα συμβόλαια προσφέρουν ένα ασφαλές περιβάλλον εκτέλεσης, αποτρέποντας απάτη, παραβιάσεις συμφωνιών ή την ανάγκη για αξιοπιστία προς τρίτους. Το επίπεδο αυτό λειτουργεί ως ενδιάμεσο ανάμεσα στα δεδομένα και τις αποκεντρωμένες εφαρμογές, επιτρέποντας τη δημιουργία λειτουργικών μοντέλων χωρίς κεντρικά σημεία ελέγχου [5].

2.1.4.6 Επίπεδο Κινήτρων (Incentives Layer)

Το επίπεδο κινήτρων είναι υπεύθυνο για τον σχεδιασμό των οικονομικών μηχανισμών που ενθαρρύνουν τη συμμετοχή στο δίκτυο και την ορθή συμπεριφορά των κόμβων [5]. Αποτελεί την αρχιτεκτονική βάση πάνω στην οποία στηρίζονται τα συστήματα ανταμοιβών και ποινών, ώστε να εξασφαλίζεται ότι οι συμμετέχοντες υποστηρίζουν τη λειτουργία του blockchain με τρόπο που ευθυγραμμίζεται με τα συμφέροντα του δικτύου.

Στο πλαίσιο PoW, οι miners ανταμείβονται για την επίλυση των κρυπτογραφικών προβλημάτων που απαιτούνται για την εξόρυξη νέων blocks, ενώ στο PoS ανταμείβονται όσοι δεσμεύουν κρυπτονομίσματα συμβάλλοντας στην ασφάλεια της διαδικασίας συναίνεσης. Εφαρμόζονται επίσης μηχανισμοί ποινών, όπως η αφαίρεση μέρους του staking (slashing), για την αποτροπή κακόβουλων ενεργειών ή λαθών που θα μπορούσαν να διαταράξουν τη λειτουργία του δικτύου.

Τα κίνητρα, επομένως, δεν αποτελούν απλώς μια οικονομική πρόβλεψη, αλλά θεμελιώδη παράγοντα για τη διατήρηση της ασφάλειας και της ακεραιότητας ενός blockchain, ευθυγραμμίζοντας τη συμπεριφορά των κόμβων με την ομαλή λειτουργία του συστήματος [5].

2.1.4.7 Επίπεδο Εφαρμογών (Application Layer)

Το επίπεδο εφαρμογών βρίσκεται στην κορυφή της αρχιτεκτονικης και αφορά όλες τις αποκεντρωμένες εφαρμογές (DApps) που χρησιμοποιούν οι τελικοί χρήστες. Το επίπεδο αυτό δεν περιγράφει τη λειτουργία των έξυπνων συμβολαίων, αλλά τον τρόπο με τον οποίο οι εφαρμογές αξιοποιούν τη λογική τους για την παροχή υπηρεσιών [5].

Στο επίπεδο εφαρμογών συναντώνται διάφορα συστήματα που καλύπτουν πραγματικές ανάγκες, όπως χρηματοοικονομικές εφαρμογές (DeFi), μητρώα ταυτότητας, συστήματα διακυβέρνησης, εφαρμογές στην εφοδιαστική αλυσίδα, στην υγεία, στην ασφάλιση και στην παρακολούθηση περιουσιακών στοιχείων. Οι εφαρμογές αυτές χρησιμοποιούν τις δυνατότητες του blockchain όπως η ακεραιότητα, η διαφάνεια και η ανθεκτικότητα ώστε να παρέχουν υψηλό επίπεδο αξιοπιστίας.

Το Application Layer συγκεντρώνει όλες τις αλληλεπιδράσεις του χρήστη με το σύστημα και αποτελεί το επίπεδο όπου η τεχνολογία του blockchain λαμβάνει πρακτική μορφή. Η πρόσβαση στις λειτουργίες του γίνεται μέσω διεπαφών χρήστη ή API, και η σύνδεση με τα έξυπνα συμβόλαια γίνεται πάντα στο παρασκήνιο, χωρίς να αναλύεται εδώ η εσωτερική λειτουργία των smart contracts. Με αυτόν τον τρόπο το επίπεδο εφαρμογών μετατρέπει τις δυνατότητες του blockchain σε πρακτικές λύσεις και υπηρεσίες που μπορούν να χρησιμοποιηθούν σε πραγματικά περιβάλλοντα [5].

2.1.5 Αρχιτεκτονικές Προκλήσεις και Μελλοντικές Ευκαιρίες

2.1.5.1 Περιορισμοί και Σφάλματα Εισόδου

Αν και το blockchain εγγυάται την ακεραιότητα των καταγεγραμμένων δεδομένων, δεν διασφαλίζει την ορθότητα ή την ποιότητα των πληροφοριών που εισάγονται. Σφάλματα στην είσοδο των δεδομένων παραμένουν αποθηκευμένα στο σύστημα και διαμοιράζονται σε όλο το δίκτυο. Παρά το ότι το συγκεκριμένο ζήτημα δεν εμπίπτει στο αντικείμενο της παρούσας μελέτης, αξίζει να σημειωθεί για λόγους πληρότητας.

2.1.5.2 Αρχιτεκτονικές Προκλήσεις

Η τεχνολογία blockchain, αν και προσφέρει ένα αξιόπιστο και ασφαλές πλαίσιο για ασφαλείς αποκεντρωμένες συναλλαγές, παρουσιάζει προκλήσεις σε αρχιτεκτονικό επίπεδο. Οι κύριες προκλήσεις σχετίζονται με την κλιμάκωση, την κατανάλωση ενέργειας και τη δυνατότητα εφαρμογής.

Σύμφωνα με τους Abrar και Sheikh [5], το blockchain (ανάλογα βέβαια με το είδος του) είναι λιγότερο κλιμακώσιμο σε σχέση με τα παραδοσιακά κεντρικοποιημένα συστήματα πληρωμών. Η αποκέντρωση ενώ ενισχύει την ασφάλεια και την ανθεκτικότητα του δικτύου, επιφέρει υψηλότερη

πολυπλοκότητα και κόστη στην ανάπτυξη και συντήρηση. Παραλληλα, συνοδεύεται από υψηλό κόστος σε ταχύτητα, καθώς το δίκτυο πρέπει να επαληθεύει κάθε συναλλαγή μέσω μηχανισμών συναίνεσης, όπως ο Proof of Work (PoW). Αυτή η διαδικασία είναι ενεργοβόρα και περιβαλλοντικά μη βιώσιμη σε μεγάλες κλίμακες, οδηγώντας στην ανάγκη μετάβασης σε πιο αποδοτικούς μηχανισμούς. Εν κατακλείδι, η αποδοτικότητα της αποκέντρωσης εξαρτάται από το αν η βασιζόμενη αρχιτεκτονική μπορεί να υλοποιηθεί άμεσα, και υποδηλώνει ότι η αποκέντρωση έχει το δικό της τίμημα, καθώς τα συστήματα πρέπει να είναι τεχνικά ώριμα για να υποστηρίξουν την απαιτούμενη ευελιξία.

2.1.5.3 Αρχιτεκτονικές λύσεις

Τα συστήματα blockchain που επιδιώκουν την εξισορρόπηση κλιμάκωσης και ασφάλειας προσπαθούν να είναι όσο το δυνατόν πιο αποδοτικά, δηλαδή ασφαλή και ουσιαστικά αποκεντρωμένα [5]. Τέτοιες προκλήσεις οδηγούν τους ερευνητές να αναζητούν λύσεις, πειραματιζόμενοι με την τροποποίηση της δομής των επιπέδων του blockchain, την υιοθέτηση εναλλακτικών μηχανισμών συναίνεσης και τη μελέτη πιθανών λύσεων.

Ο αλγόριθμος PoS, για παράδειγμα, έχει προταθεί ως εναλλακτική στο PoW, καθώς απαιτεί λιγότερους υπολογιστικούς πόρους. Επιπλέον, λύσεις όπως το Layer-2 (π.χ., Lightning Network) μεταφέρουν τις καθημερινές συναλλαγές εκτός της κύριας αλυσίδας (off-chain), μειώνοντας την επιβάρυνση του blockchain και επιταχύνοντας την επεξεργασία συναλλαγών.

Πιο αναλυτικά, η ιδέα πίσω από τις λύσεις Layer-2 (όπως το Lightning Network) είναι να αποφορτίσουν το κύριο δίκτυο του blockchain από μικρές, συχνές συναλλαγές (microtransactions), που μπορεί να είναι αργές και ακριβές λόγω της αυξημένης επιβάρυνσης του δικτύου. Αυτό σημαίνει ότι, τα κανάλια επιτρέπουν στους χρήστες να πραγματοποιούν πολλές μικροσυναλλαγές μεταξύ τους, χωρίς να πρέπει να καταγράφουν κάθε μία από αυτές στο κύριο blockchain. Αντίθετα, στο blockchain αποθηκεύεται μόνο η έναρξη και η λήξη του καναλιού πληρωμών, καθώς και οι τελικές καταστάσεις των χρημάτων που απομένουν στο κανάλι πληρωμών μεταξύ των χρηστών. Ο όρος Layer-2 προέρχεται από την έννοια ότι αυτό το επίπεδο "κάθεται" πάνω από το βασικό επίπεδο blockchain (Layer-1). Αν έπρεπε να το τοποθετήσουμε μέσα στην αρχιτεκτονική που έχει προαναφερθεί, το Layer-2 θα μπορούσε να θεωρηθεί ως ένα ενδιάμεσο επίπεδο μεταξύ του επιπέδου των δεδομένων και του επιπέδου εφαρμογής.

Με τέτοιες καινοτομίες όπως τις προαναφερόμενες, το blockchain θα μπορέσει να επεκταθεί σε πολλούς τομείς, επιλύοντας τα τρέχοντα προβλήματα και δημιουργώντας συστήματα που θα είναι βιώσιμα, επεκτάσιμα, αποκεντρωμένα, φιλικά προς το περιβάλλον και οικονομικά δικαιολογημένα [5]. Παρά τις προκλήσεις, οι μελλοντικές προοπτικές του blockchain είναι πολλά υποσχόμενες. Με την ανάπτυξη πιο βιώσιμων και αποδοτικών μηχανισμών συναίνεσης, την ενσωμάτωση αρχιτεκτονικών επιπέδων, όπως το Layer-2, και την προσαρμογή σε συγκεκριμένες απαιτήσεις εφαρμογών ανάλογα τις ανάγκες της κάθε εφαρμογής (όπως η επιλογή της αρχιτεκτονικής ή του μηχανισμού συναίνεσης που θα χρησιμοποιηθεί), το blockchain μπορεί να

επεκταθεί σε τομείς όπως τα χρηματοοικονομικά, η υγειονομική περίθαλψη και η διακυβέρνηση. Ορισμένες λύσεις από αυτές μπορούν να ενσωματωθούν σε προσαρμοσμένα επίπεδα της αρχιτεκτονικής, προσφέροντας μεγαλύτερη ευελιξία και απόδοση. Ενώ οι πιο καλές, θα χρησιμοποιηθούν σε υπάρχων επίπεδο της τρέχουσας αρχιτεκτονικής του blockchain.

2.1.6 Λειτουργικοί Ρόλοι Κόμβων στο Blockchain

Το δίκτυο blockchain απαρτίζεται από διαφορετικούς τύπους κόμβων, οι οποίοι αναλαμβάνουν συμπληρωματικούς ρόλους ώστε να διασφαλίζεται η λειτουργική συνοχή και η ανθεκτικότητα του συστήματος. Οι full nodes διατηρούν ένα πλήρες αντίγραφο της αλυσίδας και επαληθεύουν τοπικά την εγκυρότητα των συναλλαγών και των blocks σύμφωνα με τους κανόνες του πρωτοκόλλου, χωρίς απαραίτητα να συμμετέχουν άμεσα στη διαδικασία συναίνεσης, ενισχύοντας έτσι την αποκεντρωμένη φύση του δικτύου [4].

Η άμεση συμμετοχή στη διαδικασία συναίνεσης πραγματοποιείται από εξειδικευμένους ρόλους κόμβων. Στα συστήματα Proof-of-Work, οι miners προτείνουν νέα blocks επιλύοντας υπολογιστικά απαιτητικά κρυπτογραφικά προβλήματα, συμβάλλοντας στην ασφάλεια και στην αμεταβλητότητα του μητρώου [5]. Αντίστοιχα, στα συστήματα Proof-of-Stake, τον ρόλο της επικύρωσης αναλαμβάνουν οι validators, οι οποίοι επιλέγονται με βάση τη συμμετοχή τους στη διαδικασία staking και της οικονομικής τους δέσμευσης στο δίκτυο.

Επιπλέον, υπάρχουν light nodes, οι οποίοι δεν διατηρούν πλήρες αντίγραφο της αλυσίδας αλλά βασίζονται σε full nodes για την επαλήθευση πληροφοριών, καθώς και archive nodes, οι οποίοι αποθηκεύουν ολόκληρο το ιστορικό όλων των καταστάσεων του blockchain για λόγους ανάλυσης και διαφάνειας. Η κατανεμημένη αυτή πολυμορφία ρόλων, όπως υπογραμμίζει η σχετική βιβλιογραφία, αποτελεί θεμελιώδες χαρακτηριστικό που ενισχύει τη διαφάνεια, την ασφάλεια και τη λειτουργική συνέχεια του blockchain [4][5].

Οι διαφορετικοί αυτοί ρόλοι συνεργάζονται ώστε το σύστημα να παραμένει αξιόπιστο ακόμη και σε περιπτώσεις επιθέσεων ή τεχνικών δυσλειτουργιών. Η κατανεμημένη αυτή λειτουργία, όπως υπογραμμίζει η σχετική βιβλιογραφία, αποτελεί θεμελιώδες χαρακτηριστικό που ενισχύει τη διαφάνεια, την ασφάλεια και τη λειτουργική συνέχεια του blockchain [4][5].

Πίνακας 1: Βασικοί ρόλοι κόμβων σε δίκτυα blockchain

Τύπος Κόμβου	Ρόλος στο Δίκτυο	Συμμετοχή στη Συναίνεση

Full Node	Διατηρεί πλήρες αντίγραφο της αλυσίδας και επαληθεύει τοπικά συναλλαγές και blocks.	Όχι
Miner (PoW)	Προτείνει νέα blocks μέσω επίλυσης κρυπτογραφικών παζλ.	Ναι
Validator (PoS)	Προτείνει ή επικυρώνει blocks βάσει μηχανισμών staking.	Ναι
Light Node	Διατηρεί περιορισμένα δεδομένα και βασίζεται σε full nodes.	Όχι
Archive Node	Αποθηκεύει πλήρες ιστορικό καταστάσεων του blockchain.	Όχι
Relay / Seed Node	Υποστηρίζει διάδοση δεδομένων και σύνδεση νέων κόμβων.	Όχι

2.1.7 Εφαρμογές και Μελέτες Περίπτωσης

Το blockchain σχεδιάστηκε, όπως συχνά πιστεύεται, για τη λειτουργία των κρυπτονομισμάτων, όμως οι εφαρμογές του εκτείνονται σε πολλούς άλλους τομείς. Χάρη στις αρχές της διαφάνειας, της ασφάλειας και της αποκεντρωμένης διαχείρισης δεδομένων, μπορεί να χρησιμοποιηθεί σε τραπεζικές υπηρεσίες, στην εφοδιαστική αλυσίδα, την υγειονομική περίθαλψη και τη δημόσια διακυβέρνηση, βελτιώνοντας την αξιοπιστία και την αποτελεσματικότητα των διαδικασιών.

Η τεχνολογία αυτή έχει εξελιχθεί ραγδαία, αποτελώντας έναν αξιόπιστο μηχανισμό για την ταχεία και ασφαλή επεξεργασία δεδομένων. Όπως επισημαίνουν οι Pilkington [4] και Underwood [6], το blockchain δεν αφορά μόνο τα κρυπτονομίσματα, αλλά λειτουργεί ως εργαλείο αυτοματοποίησης και ενίσχυσης της διαφάνειας σε διάφορους κλάδους. Μέσα από συγκεκριμένες μελέτες περίπτωσης, αναδεικνύεται ο ρόλος του στην επίλυση κρίσιμων προβλημάτων, όπως η ασφαλής αρχειοθέτηση εγγράφων, η αξιόπιστη ψηφοφορία και η προστασία ιατρικών δεδομένων [6].

2.1.7.1 Χρηματοοικονομικά και Τραπεζικές Υπηρεσίες

Από την πρώτη του εφαρμογή για τη διακίνηση αποκεντρωμένων κρυπτονομισμάτων, όπως το Bitcoin, το blockchain έχει μετασχηματίσει τον τομέα των χρηματοοικονομικών υπηρεσιών. Χωρίς την ανάγκη μεσολάβησης από τράπεζες ή άλλους διαχειριστές πληρωμών, το blockchain καθιστά τις συναλλαγές πιο ομαλές, αξιόπιστες και οικονομικά αποδοτικές, ιδιαίτερα για διεθνείς συναλλαγές. Το δημόσιο μητρώο του blockchain μειώνει τον κίνδυνο κακόβουλης διαχείρισης των δεδομένων των συναλλαγών, ενισχύοντας την ασφάλεια, περιορίζοντας τις απάτες και μειώνοντας το κόστος συναλλαγών.

Επιπλέον, το blockchain έχει τη δυνατότητα να δημιουργεί tokens που αντιπροσωπεύουν περιουσιακά στοιχεία, όπως ακίνητα ή χρηματοοικονομικά προϊόντα. Αυτά τα tokens επιτρέπουν τη διευκόλυνση των συναλλαγών και την αύξηση της ρευστότητας, καθιστώντας τη διαχείριση περιουσιακών στοιχείων πιο αποτελεσματική και προσβάσιμη.

Η χρήση του blockchain για τη διαχείριση ψηφιακών ταυτοτήτων αυτοματοποιεί διαδικασίες συμμόρφωσης, όπως αυτές που απαιτούνται για την καταπολέμηση του ξεπλύματος χρήματος (AML) και την επιβεβαίωση ταυτοτήτων (KYC).

Η εφαρμογή του blockchain στις διασυνοριακές πληρωμές επιταχύνει τις διαδικασίες και προσφέρει σημαντικές εξοικονομήσεις, τόσο για χρηματοοικονομικά ιδρύματα όσο και για καταναλωτές. Αυτό μεταφράζεται σε πιο άμεσες και ασφαλείς μεταφορές χρημάτων, εξαλείφοντας ενδιάμεσους φορείς και μειώνοντας τον χρόνο εκτέλεσης των συναλλαγών [6].

2.1.7.2 Διαχείριση Εφοδιαστικής Αλυσίδας

Το αμετάβλητο μητρώο του blockchain προσφέρει αυξημένη ορατότητα και ανιχνευσιμότητα στις εφοδιαστικές αλυσίδες. Κάθε ενέργεια και μεταβίβαση στην εφοδιαστική αλυσίδα καταγράφεται στο κοινό μητρώο, το οποίο μπορεί να ελεγχθεί για την προέλευση, την ιστορία και την επεξεργασία ενός προϊόντος. Αυτό το επίπεδο διαφάνειας είναι ιδιαίτερα σημαντικό σε κλάδους, όπως η γεωργία, η φαρμακευτική βιομηχανία και η βιομηχανία τροφίμων. Στη φαρμακευτική, για παράδειγμα, το blockchain μπορεί να επαληθεύσει τα φάρμακα, βοηθώντας στον αγώνα κατά των πλαστών σκευασμάτων [6].

2.1.7.2.1 Mediledger

Η ενσωμάτωση της τεχνολογίας blockchain στην εφοδιαστική αλυσίδα των φαρμακευτικών προϊόντων έχει επιφέρει σημαντικές βελτιώσεις όσον αφορά τη διαφάνεια και την ασφάλεια. Η πλατφόρμα MediLedger[9] [11] αποτελεί ένα από τα επιτυχημένα παραδείγματα χρήσης αυτής της τεχνολογίας, επιτρέποντας την πλήρη ιχνηλασιμότητα των φαρμάκων και των ιατρικών συσκευών από την παραγωγή έως την τελική διάθεση. Αυτό διασφαλίζει την αυθεντικότητα και την προέλευση των προϊόντων, μειώνοντας τους κινδύνους από πλαστά φάρμακα και συσκευές.

Η τεχνολογία blockchain λειτουργεί ως ένα αποκεντρωμένο και κατανεμημένο σύστημα καταγραφής συναλλαγών, προσφέροντας αμετάβλητα και αξιόπιστα δεδομένα. Αυτό επιτρέπει στους συμμετέχοντες της εφοδιαστικής αλυσίδας να παρακολουθούν σε πραγματικό χρόνο την πορεία των προϊόντων, εξασφαλίζοντας έτσι τη διαφάνεια και την ασφάλεια στις συναλλαγές. Η χρήση

[9] S. Mohammed and N. R. Panda, "Block Chain Technology in the Pharmaceutical Supply Chain: Enhancing Transparency and Security," *IJRASE*, vol. 12, no. VIII, pp. 1336-1340, Aug. 2024. [Online]. Available: https://doi.org/10.22214/ijraset.2024.64117

έξυπνων συμβολαίων (smart contracts) εξαλείφει την ανάγκη για μεσάζοντες, προσφέροντας καθαρότητα στις συμφωνίες μεταξύ αγοραστών και πωλητών.

Παρά τις προκλήσεις που αντιμετωπίζει η εφαρμογή της τεχνολογίας blockchain, όπως η ενσωμάτωσή της με υπάρχοντα συστήματα και η συμμόρφωση με ρυθμιστικά πλαίσια, τα οφέλη που προσφέρει είναι σημαντικά. Η δυνατότητα για ασφαλή και αποτελεσματική διαχείριση δεδομένων ενισχύει την αξιοπιστία της εφοδιαστικής αλυσίδας, ενώ η προστασία των ευαίσθητων πληροφοριών διασφαλίζει την ακεραιότητα των δεδομένων. Η επιτυχία πρωτοβουλιών, όπως το MediLedger, καταδεικνύει τις δυνατότητες της τεχνολογίας blockchain να επαναστατήσει τις φαρμακευτικές εφοδιαστικές αλυσίδες, προωθώντας τη συνεργασία και την εμπιστοσύνη σε παγκόσμιο επίπεδο. [11]

2.1.7.3 Δημόσια Διακυβέρνηση

Το blockchain διασφαλίζει ότι η ηλεκτρονική ψηφοφορία παραμένει αμετάβλητη, καθώς και το δημόσιο αρχείο της. Συνεπώς, οι ψηφοφόροι μπορούν να βασίζονται σε διαδικτυακά συστήματα ψηφοφορίας χωρίς κίνδυνο, ελαχιστοποιώντας τις πιθανότητες νοθείας. Παράλληλα, το Blockchain είναι σε θέση να προστατεύσει και την ιδιωτικότητα του ψηφοφόρου έτσι ώστε κανείς να μην είναι σε θέση να γνωρίζει ποιος ψηφοφόρος έδωσε ποια ψήφο, χρησιμοποιώντας τεχνικές όπως αυτή της των αποδείξεων μηδενικής γνώσης (Zero-Knowledge Proofs - ZKP) και πιο συγκεκριμένα τη μέθοδο zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) [18], η οποία επιτρέπει την επαλήθευση των συναλλαγών-ψήφων χωρίς την αποκάλυψη λεπτομερειών του ατόμου που πήρε μέρος στη διαδικασία καθώς και διασφαλίζει ότι ο ψηφοφόρος θα έχει μόνο ένα δικαίωμα ψήφου.

Με ένα απλό παράδειγμα, ο τρόπος με τον οποίο επιτυγχάνεται αυτό είναι ο εξής:

- Έστω πως σε κάθε ψηφοφόρο παρέχεται ένα μοναδικό token (one-time PIN), για παράδειγμα με SMS από το κινητό που έχει δηλώσει στο gov, το οποίο προκύπτει και είναι άμεσα συνδεδεμένο με την ταυτότητα του, ας το πούμε TokenID.

- Η μέθοδος zk-SNARKs επιβεβαιώνει τη γνησιότητα του TokenID του ψηφοφόρου, που το ανταλλάσσει με ένα άλλο τυχαίο TokenVote, το οποίο δεν συνδέεται με τον ψηφοφόρο και δε μπορεί να γίνει αντίστροφη ιχνηλάτηση (traceback) στο πρόσωπό του ***(Ιδιωτικότητα)***. Επίσης, σημειώνει ότι ο συγκεκριμένος χρήστης έχει λάβει το one-time TokenVote που του αναλογεί.

- Για να μπορέσει να ασκήσει το δικαίωμα ψήφου του, ο χρήστης πρέπει πρώτα να «εξαργυρώσει» το δικαίωμα ψήφου του με το TokenVote που του δόθηκε. Αφού ολοκληρωθεί η διαδικασία, ο χρήστης δεν μπορεί να ξαναψηφίσει εφόσον δεν έχει άλλο TokenID και κατ' επέκταση TokenVote, εξασφαλίζοντας έτσι την ***αμεταβλητότητα*** της διαδικασίας [18].

Το blockchain παρέχει επίσης βελτιωμένη διαφάνεια σε διαδικασίες της δημόσιας διοίκησης, καθιστώντας τις ασφαλείς και ανοιχτές, με εύκολη πρόσβαση σε ένα δημόσιο αρχείο όλων των δραστηριοτήτων (των διαδικασιών) του δημόσιου τομέα. Επιπλέον, δεν χρησιμοποιείται μόνο για την καταγραφή των διαδικασιών αυτών, αλλά και για την παρακολούθηση και καταγραφή της εκτέλεσής τους. Αυτό σημαίνει ότι μπορεί να αποθηκεύει πότε, πώς και από ποιον εκτελέστηκε μια συγκεκριμένη διαδικασία, γεγονός που ενισχύει τη λογοδοσία και την αξιοπιστία. Η δυνατότητα αυτή αποτρέπει τυχόν αυθαίρετες αλλαγές ή παραλείψεις, ενώ ταυτόχρονα διασφαλίζει ότι οι διαδικασίες τηρούνται όπως προβλέπεται. Έτσι, το blockchain όχι μόνο αυξάνει τη διαφάνεια αλλά συμβάλλει και στην αποτελεσματικότερη λειτουργία της δημόσιας διοίκησης, ενισχύοντας τη δημοκρατία [6].

2.1.7.4 Υγεία

2.1.7.2.1 Ηλεκτρονικά Ιατρικά Αρχεία (EHRs) με Προσανατολισμό στον Ασθενή

Τα υπάρχοντα συστήματα υγείας περιέχουν συχνά "σιλό πληροφοριών", δηλαδή όχι ευκόλως κοινόχρηστα ή προσβάσιμα δεδομένα, με αποτέλεσμα την έλλειψη ανταλλαγής και διαλειτουργικότητας δεδομένων. Ευτυχώς, έχει προταθεί ένα νέο πρότυπο για τα EHRs, το Medicalchain[10] [7], το οποίο επικεντρώνεται στον ασθενή και είναι χαμηλού κόστους. Ειδικότερα, αντί να είναι απλά αρχεία, τα EHRs υιοθετούν ένα πρότυπο μορφοποίησης και περιεχομένου που ενσωματώνει τα δεδομένα του ασθενούς με τη χρήση έξυπνων συμβολαίων, εξασφαλίζοντας έτσι την ασφαλή διάθεση και ανταλλαγή των πληροφοριών όταν πληρούνται συγκεκριμένες προϋποθέσεις. Αυτό επιτρέπει στους ασθενείς να ελέγχουν τα δεδομένα τους και να τα κοινοποιούν με ασφάλεια και ευκολία σε οποιονδήποτε επαγγελματία υγείας. Αυτό το μοντέλο αντιμετωπίζει τις ανησυχίες για την ιδιωτικότητα των δεδομένων και την εμπιστοσύνη, ενώ διευκολύνει την ανταλλαγή πληροφοριών. [7]

2.1.7.2.2 Επαλήθευση Πιστοποιήσεων Ιατρικού Προσωπικού

Η φήμη των επαγγελματιών υγείας είναι κρίσιμη, και η διαδικασία επαλήθευσης αποτελεί βασική προϋπόθεση για την παροχή ασφαλούς φροντίδας. Το blockchain διασφαλίζει την εγκυρότητα των πιστοποιήσεων και το ιστορικό των ιατρών, επιτρέποντας στα νοσοκομεία να επαληθεύουν εύκολα τα προσόντα των επαγγελματιών υγείας χωρίς την ανάγκη επικοινωνίας με προηγούμενους εργοδότες τους [7].

2.1.7.2.3 Ασφάλεια IoT για Απομακρυσμένη Παρακολούθηση Ασθενών

Η ανάπτυξη συσκευών IoT στον τομέα της υγείας επιτρέπει την απομακρυσμένη παρακολούθηση ασθενών, αλλά τα δεδομένα παρακολούθησης πρέπει να αποθηκεύονται με ασφάλεια. Το blockchain, ως

[10] Medicalchain — Blockchain platform for secure electronic health records.
Available at: https://medicalchain.com

αμετάβλητο πλαίσιο, επιτρέπει την ασφαλή αποθήκευση και διαθεσιμότητα των δεδομένων IoT, βελτιώνοντας την προστασία της ιδιωτικότητας και την ποιότητα της περίθαλψης [7].

Το blockchain έχει τη δυνατότητα να αντιμετωπίσει θεμελιώδεις προκλήσεις στον τομέα της υγείας, όπως η ασφάλεια των δεδομένων, η διαφάνεια και η βελτίωση των επιχειρησιακών διαδικασιών. Μέσω της ενοποίησης διαφορετικών συστημάτων και της μείωσης της πολυπλοκότητας, το blockchain συμβάλλει στην αποφυγή ανθρώπινων λαθών και στην αυτοματοποίηση των πολύπλοκων επιχειρησιακών διαδικασιών, εξασφαλίζοντας έτσι ακρίβεια και αξιοπιστία. Όλα αυτά οδηγούν σε αυξημένη παρουσία του blockchain στο χώρο της υγειονομικής περίθαλψης, ενισχύοντας την αποτελεσματικότητα των συστημάτων και βελτιώνοντας την ποιότητα της φροντίδας που παρέχεται στους ασθενείς.

2.1.8 Διαδικασία Επικύρωσης και Ροή Συναλλαγών στο Blockchain

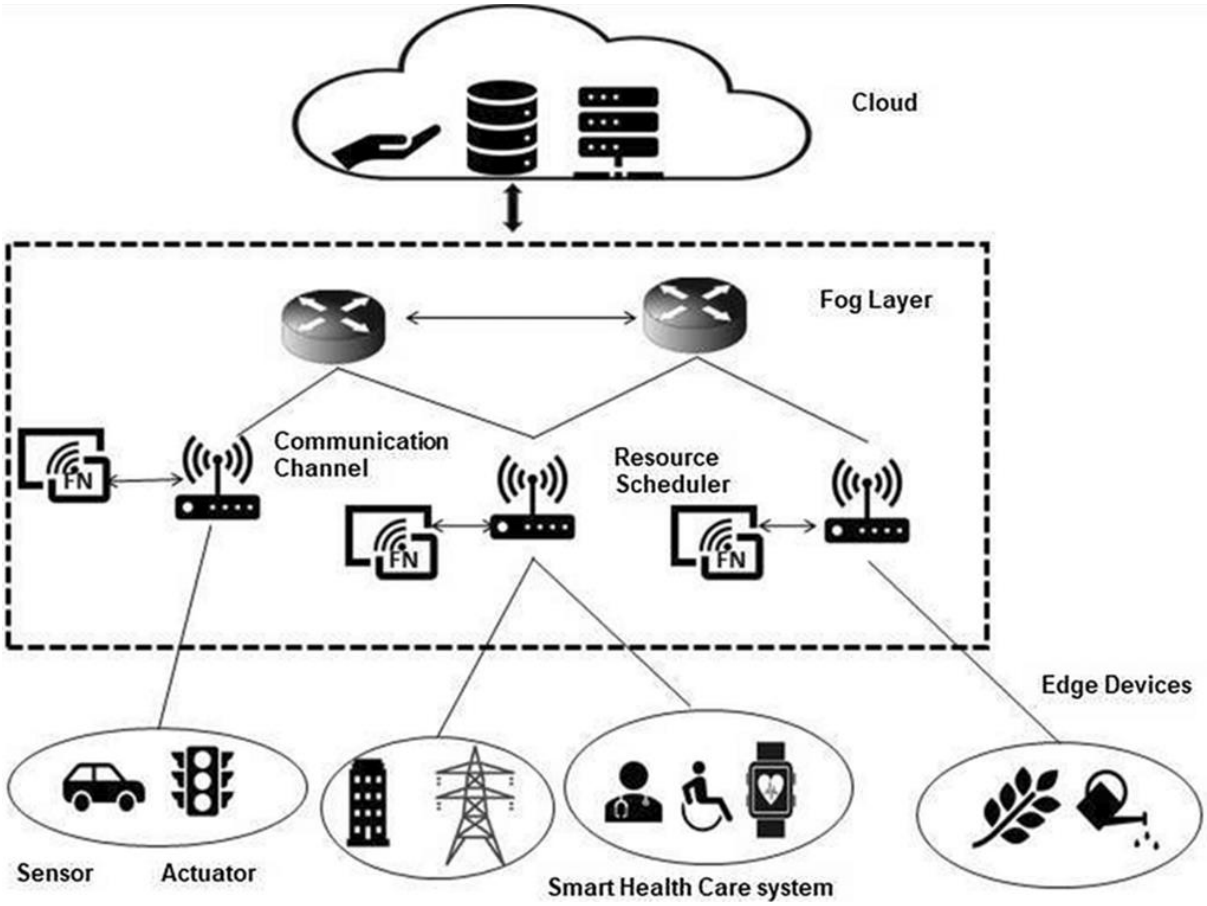
Η διαδικασία επικύρωσης μιας συναλλαγής στο blockchain διασφαλίζει ότι κάθε καταγραφή που προστίθεται στο κατανεμημένο μητρώο είναι έγκυρη και σύμφωνη με τους κανόνες του πρωτοκόλλου. Όπως περιγράφεται στη σχετική βιβλιογραφία, η ακεραιότητα των συναλλαγών επιτυγχάνεται μέσω κρυπτογραφικών μηχανισμών και αποκεντρωμένης επαλήθευσης [4,5]. Αρχικά, ο αποστολέας δημιουργεί τη συναλλαγή και την υπογράφει με το ιδιωτικό του κλειδί, εξασφαλίζοντας ότι μόνο ο νόμιμος κάτοχος μπορεί να την εξουσιοδοτήσει. Η συναλλαγή αποστέλλεται έπειτα στο δίκτυο και τοποθετείται στο mempool, όπου παραμένει μέχρι να αξιολογηθεί από τους κόμβους του συστήματος.

Οι κόμβοι επαλήθευσης εξετάζουν την εγκυρότητα της ψηφιακής υπογραφής, την επάρκεια των διαθέσιμων πόρων (όπως το διαθέσιμο υπόλοιπο και τα απαιτούμενα τέλη συναλλαγής), καθώς και τη συμμόρφωση της συναλλαγής με το πρωτόκολλο, όπως το ότι ακολουθεί τη σωστή δομή και μορφή, και δεν παραβιάζει κανόνες όπως διπλή δαπάνη [4]. Οι έγκυρες συναλλαγές ομαδοποιούνται σε ένα υποψήφιο block, το οποίο υποβάλλεται προς προσθήκη στην αλυσίδα μέσω του κατάλληλου μηχανισμού συναίνεσης, όπως το Proof-of-Work ή το Proof-of-Stake [5].

Πέρα από τους επιμέρους ελέγχους επικύρωσης, ιδιαίτερη σημασία έχει και η συνολική ροή δεδομένων από τη δημιουργία μιας συναλλαγής έως την ενσωμάτωσή της σε block. Κατά τη δημιουργία ενός block, ο κόμβος που συμμετέχει στη διαδικασία συναίνεσης επιλέγει συναλλαγές από το mempool, τις ταξινομεί και υπολογίζει τη ρίζα Merkle, η οποία διασφαλίζει την ακεραιότητα όλων των επιμέρους εγγραφών [5].

Αφού επιτευχθεί συναίνεση, το προτεινόμενο block διαδίδεται στο δίκτυο και επαληθεύεται ανεξάρτητα από κάθε κόμβο ως προς την εγκυρότητα των συναλλαγών και τη συμμόρφωσή του με τους κανόνες του πρωτοκόλλου. Ύστερα, το block προστίθεται στην αλυσίδα και η νέα κατάσταση διαδίδεται σε όλους τους κόμβους του δικτύου, εξασφαλίζοντας συνεκτική και αδιάβλητη ενημέρωση του καθολικού [4].

2.2. Τι είναι ο Ομιχλώδης Υπολογισμός (Fog Computing)



Εικόνα 2: Αρχιτεκτονική του fog computing [13].

2.2.1 Ορισμός

Ο ομιχλώδης υπολογισμός (fog computing) είναι μια κατανεμημένη υπολογιστική αρχιτεκτονική που λειτουργεί ως ενδιάμεσο επίπεδο ανάμεσα στο υπολογιστικό νέφος και τις τελικές συσκευές (edge devices). Εισήχθη από την Cisco για την κάλυψη των αναγκών επεξεργασίας δεδομένων σε πραγματικό χρόνο, μειώνοντας την εξάρτηση από απομακρυσμένα αλλά κεντρικοποιημένα κέντρα δεδομένων (του υπολογιστικού νέφους). Ο ομιχλώδης υπολογισμός διαχειρίζεται δεδομένα τοπικά, αυξάνοντας την αποδοτικότητα και μειώνοντας τις καθυστερήσεις [2].

2.2.2 Χαρακτηριστικά και Πλεονεκτήματα του Fog Computing

2.2.2.1 Κατανεμημένη Επεξεργασία

Ο ομιχλώδης υπολογισμός (fog computing) βασίζεται σε μια κατανεμημένη αρχιτεκτονική που ενσωματώνει κόμβους επεξεργασίας (fog nodes) κοντά στις πηγές των δεδομένων, όπως είναι οι συσκευές IoT. Αυτοί οι κόμβοι συνήθως

υλοποιούνται ως ενδιάμεσες δικτυακές και υπολογιστικές συσκευές, όπως edge servers, βιομηχανικές πύλες (IoT gateways), δρομολογητές/routers με υπολογιστικές δυνατότητες, ή ακόμη και μικροδιακομιστές (micro-servers) εγκατεστημένοι σε τοπικά δίκτυα (π.χ. σε εργοστάσια, νοσοκομεία ή υποδομές έξυπνων πόλεων). Σε αντίθεση με το cloud, οι κόμβοι αυτοί βρίσκονται γεωγραφικά κοντά στις πηγές δεδομένων και λειτουργούν ως ενδιάμεσο επίπεδο μεταξύ edge συσκευών και υπολογιστικού νέφους. Η κατανεμημένη αυτή προσέγγιση μειώνει την εξάρτηση από απομακρυσμένα κέντρα δεδομένων, ενώ παράλληλα διασφαλίζει την τοπική επεξεργασία, φιλτράρισμα και αποθήκευση δεδομένων πριν αυτά σταλούν στο νέφος για πιο απαιτητική ανάλυση [17], [5].

Οι κόμβοι ομίχλης (fog nodes) ενσωματώνουν τεχνολογίες, όπως εικονικοποίηση (virtualization) και δοχειοποίηση (containerization), που επιτρέπουν την ταυτόχρονη εκτέλεση πολλαπλών εφαρμογών. Με αυτόν τον τρόπο, οι διαθέσιμοι πόροι αξιοποιούνται στο μέγιστο, αυξάνοντας τη λειτουργική αποδοτικότητα του συστήματος [17].

2.2.2.2 Ευελιξία και Κλιμακωσιμότητα

Η κατανεμημένη φύση του fog computing ενισχύει και την ευελιξία της υποδομής, καθώς το σύστημα μπορεί να προσαρμόζεται δυναμικά σε διαφορετικές απαιτήσεις εφαρμογών. Οι υποδομές ομίχλης είναι εγγενώς επεκτάσιμες: αφενός, μπορούν να ενισχυθούν με την προσθήκη νέων κόμβων ώστε να καλύψουν αυξανόμενες ανάγκες· αφετέρου, οι ίδιες οι εφαρμογές μπορούν να κλιμακωθούν καθώς αντλούν πόρους από το σύνολο της υποδομής, όποτε και όπου απαιτείται. Αυτή η δυνατότητα δυναμικής εκχώρησης υπολογιστικών και αποθηκευτικών πόρων καθιστά το fog computing ιδιαίτερα κατάλληλο για μεταβαλλόμενα περιβάλλοντα, όπως οι έξυπνες πόλεις ή οι αυτοματοποιημένες βιομηχανικές μονάδες [17].

Η συνδυαστική δράση ενεργειακής αποδοτικότητας, μηχανισμών ασφάλειας και λειτουργικής ευελιξίας επιβεβαιώνει ότι το fog computing δεν αποτελεί μόνο μια υποστηρικτική τεχνολογία για το cloud, αλλά μια αυτόνομη και στρατηγικά κρίσιμη επιλογή για εφαρμογές που απαιτούν χαμηλή καθυστέρηση, υψηλή διαθεσιμότητα και ισχυρή προστασία των δεδομένων.

2.2.2.3 Αλγόριθμοι Διαχείρισης Φορτίου

Η κατανεμημένη επεξεργασία δεδομένων στο fog computing απαιτεί την εφαρμογή αλγορίθμων διαχείρισης φορτίου (load balancing) για την αποτελεσματική κατανομή των πόρων ανάμεσα στους κόμβους ομίχλης. Οι αλγόριθμοι αυτοί χρησιμοποιούνται για να εξασφαλίσουν την ισότιμη κατανομή του φόρτου εργασίας, αποφεύγοντας την υπερφόρτωση συγκεκριμένων κόμβων και βελτιώνοντας την απόδοση του συστήματος. Ο σκοπός είναι να επιτευχθεί υψηλή αποδοτικότητα και να μειωθεί η καθυστέρηση στη διαδικασία επεξεργασίας των δεδομένων. Αυτός ο τύπος διαχείρισης φορτίου είναι

απαραίτητος για συστήματα με υψηλές απαιτήσεις, όπως τα δίκτυα IoT, όπου η απόκριση σε πραγματικό χρόνο είναι κρίσιμη.

Για παράδειγμα, ένας από τους πιο διαδεδομένους και απλούστερους αλγόριθμους διαχείρισης φορτίου είναι ο Round Robin, ο οποίος κατανέμει τις εργασίες κυκλικά μεταξύ των διαθέσιμων κόμβων. Με αυτόν τον τρόπο, οι κόμβοι που δεν είναι υπό καθεστώς υπερφόρτωσης αναλαμβάνουν την εκτέλεση νέων εργασιών, μειώνοντας την πιθανότητα υπερφόρτωσης ενός συγκεκριμένου κόμβου και ενισχύοντας τη συνολική ισορροπία του συστήματος. Ο παραπάνω αλγόριθμος, αν και προσφέρει μια στοιχειώδη μορφή εξισορρόπησης, δεν λαμβάνει υπόψη τη διακύμανση στον υπολογιστικό φόρτο κάθε αιτήματος, γεγονός που μπορεί να οδηγήσει σε ανισορροπία όταν ορισμένοι κόμβοι επιφορτιστούν με πιο απαιτητικές διεργασίες [17].

Ένας ελαφρώς πιο προσαρμοστικός αλγόριθμος είναι ο Least Connections, ο οποίος χρησιμοποιείται συχνά σε ομιχλώδη συστήματα και βασίζεται στην κατανομή της εργασίας στον κόμβο που έχει τον λιγότερο αριθμό ενεργών συνδέσεων. Αν και ο αριθμός των συνδέσεων μπορεί να λειτουργήσει ως πρόχειρος δείκτης του φόρτου εργασίας ενός κόμβου, η μεθοδολογία αυτή δεν υπολογίζει με ακρίβεια το ποσοτικό και ποιοτικό βάρος κάθε σύνδεσης. Συνεπώς, η κατανομή παραμένει κατά προσέγγιση και όχι απολύτως βελτιστοποιημένη [5].

Οι πιο εξεζητημένοι αλγόριθμοι διαχείρισης φόρτου λαμβάνουν υπόψη διάφορους παράγοντες κατά τη διαδικασία της κατανομής των πόρων, όπως:

- η γεωγραφική θέση των κόμβων προς τις πηγές δεδομένων ή τους τελικούς χρήστες,
- η πραγματική υπολογιστική επιβάρυνση που έχει κάθε κόμβος σε πραγματικό χρόνο,
- και η συνδεσιμότητα ή το διαθέσιμο εύρος ζώνης κάθε δικτυακού κόμβου [17].

Οι μέθοδοι αυτές αξιοποιούν μετρικές runtime (π.χ. latency, CPU usage, memory load) και απαιτούν συνεχείς μηχανισμούς παρακολούθησης και ανατροφοδότησης (monitoring/feedback loops) ώστε να ανανεώνουν την κατανομή με βάση τα πραγματικά δεδομένα φόρτου.

Επιπλέον, η χρήση τεχνολογιών όπως η εικονικοποίηση (virtualization) και η δοχειοποίηση (containerization) προσφέρει τη δυνατότητα για αποδοτική συνεκτέλεση πολλαπλών εφαρμογών στους ίδιους φυσικούς πόρους. Αυτό επιτρέπει την ευέλικτη προσαρμογή της κατανομής φόρτου με βάση τις ανάγκες κάθε εφαρμογής, αυξάνοντας έτσι τη συνολική αποδοτικότητα και αξιοπιστία των fog συστημάτων [17].

Συνολικά, η ενσωμάτωση κατάλληλων αλγορίθμων διαχείρισης φορτίου στα fog περιβάλλοντα είναι κρίσιμη για τη σταθερή λειτουργία και την επεκτασιμότητα των κατανεμημένων υποδομών. Ιδίως σε εφαρμογές με αυξημένες απαιτήσεις διαθεσιμότητας και χαμηλού latency, όπως τα βιομηχανικά συστήματα αυτοματοποίησης και οι ευαίσθητες υπηρεσίες στις έξυπνες πόλεις, η χρήση των αλγορίθμων αυτών δεν αποτελεί πολυτέλεια αλλά αναγκαιότητα [5].

2.2.2.4 Πρωτόκολλα Επικοινωνίας

Η επικοινωνία στο fog computing βασίζεται στη χρήση πρωτοκόλλων χαμηλής καθυστέρησης, όπως το MQTT και το CoAP. Αυτά τα πρωτόκολλα έχουν σχεδιαστεί ειδικά για συστήματα περιορισμένων πόρων, επιτρέποντας την ανταλλαγή δεδομένων σε πραγματικό χρόνο με υψηλή αποδοτικότητα. Χρησιμοποιούνται ευρέως σε εφαρμογές IoT, όπου απαιτείται αδιάλειπτη επικοινωνία και χαμηλή καθυστέρηση [17].

2.2.2.5 Μείωση Καθυστερήσεων

Το fog computing μειώνει δραστικά την καθυστέρηση (latency), μεταφέροντας την επεξεργασία δεδομένων σε κόμβους που βρίσκονται πλησιέστερα στις πηγές παραγωγής τους. Η εγγύτητα αυτή επιτρέπει άμεση λήψη αποφάσεων και απόκριση σε πραγματικό χρόνο, περιορίζοντας την ανάγκη συνεχούς αποστολής δεδομένων στο κεντρικό νέφος (cloud), κάτι που είναι κρίσιμο σε εφαρμογές όπου ακόμη και μικρές καθυστερήσεις μπορούν να επηρεάσουν το αποτέλεσμα, όπως η αυτόνομη οδήγηση, οι βιομηχανικοί αυτοματισμοί, η υγειονομική περίθαλψη και τα έξυπνα ενεργειακά δίκτυα.

Η τοπική επεξεργασία δεδομένων από αισθητήρες σε επίπεδο fog μειώνει τον χρόνο μετάδοσης και επιταχύνει την ενεργοποίηση μηχανισμών ελέγχου σε κρίσιμες συνθήκες, ενώ η υιοθέτηση κατανεμημένων αλγορίθμων επεξεργασίας και εντοπισμένης ανάλυσης στα σημεία παραγωγής δεδομένων περιορίζει τη μεταφορά φορτίου και υποστηρίζει αυτοματοποιημένη διαχείριση συμβάντων με ελάχιστη χρονική υστέρηση [5]. Επιπλέον, η χρήση ελαφριών πρωτοκόλλων επικοινωνίας, όπως τα MQTT και CoAP, διευκολύνει την ανταλλαγή δεδομένων με χαμηλό overhead και συμβάλλει περαιτέρω στη μείωση της καθυστέρησης [17], [5].

2.2.2.6 Ενεργειακή Αποδοτικότητα

Η τοπική επεξεργασία δεδομένων στους κόμβους ομίχλης μειώνει την ανάγκη για μαζική μεταφορά δεδομένων στο υπολογιστικό νέφος, με αποτέλεσμα να μειώνεται η συνολική κατανάλωση ενέργειας του συστήματος. Η τοπική ανάλυση και φιλτράρισμα των πληροφοριών πριν αποσταλούν, καθιστούν τους κόμβους ομίχλης κάτι περισσότερο από απλούς μεσάζοντες, καθώς αποκτούν ενεργό ρόλο στην υπολογιστική διαδικασία, βελτιώνοντας την ενεργειακή αποδοτικότητα της υποδομής συνολικά. Επιπλέον, οι κόμβοι ομίχλης ενσωματώνουν κατάλληλες τεχνικές ή μεθόδους διαχείρισης ενέργειας, όπως η χρήση χαμηλής κατανάλωσης επεξεργαστών και η λειτουργία σε "sleep mode" όταν δεν χρησιμοποιούνται [5].

Η ενεργειακή απόδοση ενισχύεται περαιτέρω όταν οι παραπάνω πρακτικές συνδυάζονται με κατάλληλους αλγόριθμους κατανομής φόρτου. Όταν το συνολικό σύστημα λειτουργεί με χαμηλό φόρτο, η δυνατότητα συγκέντρωσης της υπολογιστικής δραστηριότητας σε ένα υποσύνολο κόμβων επιτρέπει σε άλλους να παραμένουν ανενεργοί, μειώνοντας την κατανάλωση χωρίς να επηρεάζεται η απόδοση. Αυτή η στρατηγική έχει υιοθετηθεί επιτυχώς σε

σύγχρονα κέντρα δεδομένων και μπορεί να εφαρμοστεί αντίστοιχα και στο περιβάλλον ομίχλης [17].

2.2.2.7 Ασφάλεια και Προστασία Ιδιωτικότητας

Σε ό,τι αφορά την ασφάλεια και την προστασία ιδιωτικότητας, το fog computing προσφέρει σημαντικά πλεονεκτήματα χάρη στην αποκεντρωμένη φύση του. Η τοπική αποθήκευση και επεξεργασία δεδομένων μειώνει την ανάγκη μεταφοράς ευαίσθητων πληροφοριών σε απομακρυσμένες υποδομές, περιορίζοντας έτσι τα σημεία πιθανής παραβίασης. Η ασφάλεια διασφαλίζεται με την εφαρμογή τεχνικών, όπως η αυθεντικοποίηση χρηστών, η εξουσιοδότηση πρόσβασης, και η χρήση κρυπτογραφικών πρωτοκόλλων κατά τη μεταφορά των δεδομένων. Οι αλγόριθμοι συμμετρικής κρυπτογράφησης, όπως ο AES, προτιμώνται συχνά λόγω του χαμηλότερου ενεργειακού τους αποτυπώματος σε περιβάλλοντα περιορισμένων πόρων. Παράλληλα, η επιλεκτική κρυπτογράφηση δηλαδή η στοχευμένη προστασία μόνο κρίσιμων πεδίων ή υποσυνόλων των δεδομένων προσφέρει ισορροπία μεταξύ απόδοσης και ασφάλειας. Τέλος, δεδομένα που αποθηκεύονται τοπικά στους κόμβους ομίχλης προστατεύονται με τη χρήση κρυπτογραφημένων μορφών αποθήκευσης, ώστε να παραμένουν μη αναγνώσιμα ακόμη και σε περίπτωση φυσικής παραβίασης των κόμβων [5], [17].

Επιπλέον, η αρχιτεκτονική του fog computing επιτρέπει την εφαρμογή πολιτικών ασφάλειας σε τοπικό επίπεδο, προσαρμοσμένων στο εκάστοτε περιβάλλον λειτουργίας. Η εγγύτητα των κόμβων ομίχλης στις πηγές δεδομένων διευκολύνει τον άμεσο εντοπισμό ανωμαλιών και τη γρήγορη απόκριση σε περιστατικά ασφαλείας, χωρίς την καθυστέρηση που συνεπάγεται η επικοινωνία με απομακρυσμένα κέντρα δεδομένων. Με τον τρόπο αυτό, μειώνεται η επιφάνεια επίθεσης και ενισχύεται η ανθεκτικότητα του συστήματος απέναντι σε κακόβουλες ενέργειες, καθιστώντας το fog computing ιδιαίτερα κατάλληλο για κρίσιμες και ευαίσθητες εφαρμογές.

Τέλος, το fog computing επιτρέπει την εφαρμογή τεχνικών ανωνυμοποίησης ή ψευδωνυμοποίησης (anonymization/pseudonymization) πριν από τη μεταφορά δεδομένων στο νέφος, ώστε να μειώνεται ο κίνδυνος ταυτοποίησης χρηστών ή συσκευών. Η δυνατότητα αυτή είναι ιδιαίτερα χρήσιμη, καθώς οι fog nodes διαθέτουν περισσότερους πόρους από τις edge συσκευές και μπορούν να υποστηρίξουν πιο σύνθετες τεχνικές προστασίας ιδιωτικότητας [5].

2.2.3 Αρχιτεκτονική του Fog Computing

Η αρχιτεκτονική του fog computing είναι πολυδιάστατη και σχεδιασμένη για να υποστηρίζει κατανεμημένα συστήματα με έμφαση στην βελτιστοποίηση της απόδοσης, της ασφάλειας και της ευελιξίας. Σκοπός της είναι να γεφυρώσει το χάσμα μεταξύ των συσκευών IoT που βρίσκονται στην άκρη του δικτύου (edge) και των απομακρυσμένων κέντρων δεδομένων του υπολογιστικού νέφους, παρέχοντας τη δυνατότητα τοπικής επεξεργασίας, αποθήκευσης και ανάλυσης δεδομένων. Μέσω αυτού του μοντέλου, το fog computing μειώνει τη συνδεσιμότητα με το νέφος, επιτρέποντας την αποτελεσματικότερη διαχείριση

των δεδομένων κοντά στην πηγή τους, ενώ ταυτόχρονα ενισχύει την ασφάλεια και την ταχύτητα απόκρισης του συστήματος [2], [17].

Η επιλογή του πώς αναπτύσσεται (deployment) μια υποδομή fog αποτελεί κρίσιμο παράγοντα, διότι επηρεάζει άμεσα το επίπεδο ελέγχου, την επιφάνεια επίθεσης και τις απαιτήσεις ασφάλειας/ιδιωτικότητας του συστήματος. Σε αντίθεση με το cloud, όπου οι υπηρεσίες φιλοξενούνται συνήθως σε κεντρικά και αυστηρά ελεγχόμενα data centers, το fog computing αναπτύσσεται συχνά σε γεωγραφικά διασκορπισμένες και διοικητικά ετερογενείς υποδομές (multi-administrative domains), όπου οι κόμβοι μπορεί να ανήκουν είτε στον οργανισμό που χρησιμοποιεί την υπηρεσία είτε σε τρίτους παρόχους ή φορείς που φιλοξενούν την υποδομή [2]. Στη βιβλιογραφία διακρίνονται ενδεικτικά σενάρια όπως: (α) ανάπτυξη σε ιδιωτικές εγκαταστάσεις οργανισμών (private/enterprise fog), (β) ανάπτυξη σε δημόσιους ή ημι-δημόσιους χώρους και κοινόχρηστες υποδομές (public/shared fog), και (γ) υβριδικά μοντέλα όπου συνυπάρχουν ιδιωτικοί κόμβοι με κόμβους τρίτων (hybrid fog) [17], [5].

Κάθε μοντέλο συνεπάγεται διαφορετικές παραδοχές εμπιστοσύνης και διαφορετικό βαθμό φυσικής προστασίας, γεγονός που επηρεάζει άμεσα κινδύνους όπως φυσική παραβίαση κόμβων, μη εξουσιοδοτημένη πρόσβαση σε δεδομένα και δυσκολία επιβολής ενιαίων πολιτικών ασφάλειας. Για τον λόγο αυτό, σε deployments με περιορισμένο φυσικό έλεγχο απαιτούνται συχνά πρόσθετοι μηχανισμοί όπως secure boot, hardware root-of-trust, καταγραφή συμβάντων και απομακρυσμένη πιστοποίηση (remote attestation), ώστε να διασφαλίζεται ότι οι fog κόμβοι λειτουργούν σε αξιόπιστη κατάσταση και ότι η επεξεργασία δεδομένων πραγματοποιείται σε έμπιστα περιβάλλοντα [5].

Οι παραπάνω μηχανισμοί αναφέρονται ενδεικτικά στο πλαίσιο του υποβάθρου, ενώ η λεπτομερέστερη ανάλυση των τεχνικών ασφάλειας και των αντίστοιχων προσεγγίσεων μετριασμού παρουσιάζεται στα κεφάλαια που αφορούν την ασφάλεια και τις προτεινόμενες λύσεις.

Συνεπώς, η κατανόηση των μοντέλων ανάπτυξης αποτελεί απαραίτητο μέρος του υποβάθρου, καθώς συνδέει τη στρωματική αρχιτεκτονική του fog με τις πρακτικές παραδοχές ασφάλειας που ισχύουν στην πραγματική εγκατάσταση και λειτουργία της υποδομής.

Η αρχιτεκτονική του fog computing αποτελείται από τρία βασικά επίπεδα: το επίπεδο edge, το επίπεδο ομίχλης και το επίπεδο νέφους, τα οποία συνεργάζονται στενά για την αποδοτική διαχείριση των δεδομένων και πόρων στα πλαίσια των εφαρμογών και υπηρεσιών που εκτελούνται στο ομιχλώδες περιβάλλον. Κάθε επίπεδο έχει συγκεκριμένες λειτουργίες και παρέχει διαφορετικά πλεονεκτήματα στο σύστημα συνολικά, ενώ παράλληλα βελτιώνει την απόδοση και την ασφάλεια των εφαρμογών που το χρησιμοποιούν.

2.2.3.1 Επίπεδο Ακμής (Edge Layer)

Το πρώτο επίπεδο της αρχιτεκτονικής είναι το επίπεδο των συσκευών ακμής (edge), το οποίο περιλαμβάνει συσκευές IoT που αποτελούν την κύρια πηγή δεδομένων. Αυτές οι συσκευές, όπως αισθητήρες, κάμερες, έξυπνοι μετρητές και φορητές συσκευές (wearables), συλλέγουν δεδομένα από το περιβάλλον ή

τους χρήστες. Η επικοινωνία των συσκευών IoT με το επόμενο επίπεδο (fog) πραγματοποιείται μέσω ελαφρών ασύρματων πρωτοκόλλων, όπως το MQTT (Message Queuing Telemetry Transport) και το CoAP (Constrained Application Protocol), που είναι σχεδιασμένα για λειτουργία σε περιβάλλοντα με περιορισμένους πόρους. Η βασική τους λειτουργία είναι η αποστολή των δεδομένων στο fog layer για επεξεργασία, φιλτράρισμα και περαιτέρω αξιοποίηση. Έτσι, διαχωρίζεται καθαρά ο ρόλος των edge συσκευών ως σημείων διαίσθησης από τον ρόλο των fog κόμβων ως μονάδων επεξεργασίας, σύμφωνα με τη βασική αρχή του fog computing [17].

2.2.3.2 Επίπεδο Ομίχλης (Fog Layer)

Το επίπεδο ομίχλης αντιπροσωπεύει το ενδιάμεσο στρώμα της αρχιτεκτονικής, το οποίο βρίσκεται μεταξύ των συσκευών ακμής και του υπολογιστικού νέφους, και περιλαμβάνει κόμβους μεσαίας υπολογιστικής ισχύος. Οι κόμβοι αυτοί είναι υπεύθυνοι για την τοπική αποθήκευση, την ανάλυση και την επεξεργασία των δεδομένων που προέρχονται από τις συσκευές IoT. Συνήθως υλοποιούνται μέσω δικτυακών συσκευών, όπως δρομολογητές (routers), μεταγωγείς (switches) και εξυπηρετητές μικρής έως μεσαίας ισχύος, οι οποίοι ενσωματώνονται σε τοπικές μονάδες (mini data centers) κοντά στο σημείο παραγωγής των δεδομένων [2], [5].

Η βασική λειτουργία του fog layer είναι η προσωρινή αποθήκευση των εισερχόμενων δεδομένων, καθώς και η πραγματοποίηση πρώιμης ανάλυσης σε πραγματικό χρόνο. Πριν τα δεδομένα αποσταλούν στο υπολογιστικό νέφος για μακροπρόθεσμη αποθήκευση ή περαιτέρω επεξεργασία, υφίστανται έναν αρχικό διαχωρισμό (φιλτράρισμα), ώστε να εντοπιστούν τα κρίσιμα ή ευαίσθητα δεδομένα που απαιτούν άμεση ανάλυση ή επιπλέον μέτρα προστασίας. Αυτό το φιλτράρισμα δεν έχει τη μορφή λειτουργιών τύπου firewall, αλλά αναφέρεται σε μηχανισμούς ταξινόμησης, συμπίεσης ή απόρριψης περιττών δεδομένων, με στόχο τη βελτιστοποίηση της χρήσης των διαθέσιμων πόρων. Η διαδικασία της κρυπτογράφησης εφαρμόζεται στα δεδομένα που πρόκειται να μεταφερθούν στο cloud μετά την ολοκλήρωση της τοπικής επεξεργασίας, εξασφαλίζοντας την προστασία τους κατά τη μεταφορά και την αποθήκευσή τους σε απομακρυσμένα περιβάλλοντα. Στο πλαίσιο αυτό, μπορούν να χρησιμοποιηθούν ελαφριά σχήματα συμμετρικής κρυπτογράφησης, ώστε να επιτευχθεί ισορροπία μεταξύ ασφάλειας και ενεργειακής αποδοτικότητας [5].

Το επίπεδο ομίχλης είναι καθοριστικής σημασίας για εφαρμογές που απαιτούν ταχύτατη απόκριση και χαμηλές καθυστερήσεις, όπως η βιομηχανική αυτοματοποίηση, η έξυπνη κινητικότητα ή η απομακρυσμένη παρακολούθηση ασθενών. Η τοπική ανάλυση και διαχείριση των δεδομένων μειώνει δραστικά την εξάρτηση από το κεντρικό υπολογιστικό νέφος και συμβάλλει τόσο στη μείωση της κυκλοφορίας δεδομένων όσο και στη διατήρηση υψηλού επιπέδου ιδιωτικότητας και ασφάλειας [2].

Οι κόμβοι ομίχλης (fog nodes), που συγκροτούν το fog layer, αναλαμβάνουν επίσης τη διαχείριση της ροής δεδομένων μεταξύ των edge συσκευών και του υπολογιστικού νέφους, ελέγχοντας την κατεύθυνση και τον όγκο των δεδομένων που μεταφέρονται, ώστε να μειώνεται η συμφόρηση στο δίκτυο. Παράλληλα, μπορούν να αξιοποιούν τεχνολογίες εικονικοποίησης

(virtualization) και δοχειοποίησης (containerization), επιτρέποντας την ταυτόχρονη εκτέλεση πολλαπλών εργασιών σε έναν κόμβο και βελτιώνοντας τη συνολική αποδοτικότητα της υποδομής [17], [5].

2.2.3.3 Επίπεδο Νέφους (Cloud Layer)

Το επίπεδο νέφους, το υψηλότερο από τα τρία, παρέχει τις απαραίτητες υποδομές για την επεξεργασία και αποθήκευση μεγάλων όγκων δεδομένων. Αν και το νέφος δεν είναι άμεσα εμπλεκόμενο στην αρχική επεξεργασία δεδομένων (όπως αυτή πραγματοποιείται στο ενδιάμεσο επίπεδο), διαδραματίζει έναν καθοριστικό ρόλο στην εκτέλεση σύνθετων επεξεργασιών & αναλύσεων, όπως η ανάλυση μεγάλων δεδομένων (big data analytics). Επομένως, το νέφος διαχειρίζεται την μόνιμη αποθήκευση και επεξεργασία των δεδομένων που έχουν προηγουμένως φιλτραριστεί και προεπεξεργαστεί στους κόμβους ομίχλης, αναλαμβάνοντας πιο απαιτητικές υπολογιστικές διαδικασίες που απαιτούν εκτεταμένους πόρους. Παραδείγματα αυτών περιλαμβάνουν την εκπαίδευση μοντέλων τεχνητής νοημοσύνης, τα οποία απαιτούν υψηλή υπολογιστική ισχύ και αποθηκευτικούς πόρους που παρέχονται αποκλειστικά από το νέφος. Η συνεργασία μεταξύ των τριών επιπέδων ακμής, ομίχλης & νέφους επιτρέπει την υλοποίηση μιας ευέλικτης και αποδοτικής λύσης για εφαρμογές υψηλής απόδοσης και ασφάλειας [5].

2.2.4 Εφαρμογές του Fog Computing

Το fog computing έχει εισαχθεί ως μια καινοτόμος μεθοδολογία για την αντιμετώπιση των αυξανόμενων απαιτήσεων των σύγχρονων κατανεμημένων συστημάτων, ιδίως σε εφαρμογές που απαιτούν χαμηλή καθυστέρηση, ασφάλεια και αποδοτική διαχείριση δεδομένων. Οι δυνατότητές του το καθιστούν ιδανικό για ένα ευρύ φάσμα εφαρμογών, από το Διαδίκτυο των Πραγμάτων (IoT) έως τη βιομηχανία και τα έξυπνα δίκτυα ενέργειας.

2.2.4.1. Διαδίκτυο των Πραγμάτων (IoT)

Το fog computing διαδραματίζει πρωταγωνιστικό ρόλο στο IoT, παρέχοντας την υποδομή για την επεξεργασία δεδομένων κοντά στις πηγές τους. Οι συσκευές IoT, όπως αισθητήρες και κάμερες, παράγουν τεράστιους όγκους δεδομένων, τα οποία συχνά απαιτούν άμεση ανάλυση. Η χρήση του fog computing επιτρέπει την προεπεξεργασία αυτών των δεδομένων σε τοπικούς κόμβους fog, μειώνοντας την καθυστέρηση και τη συμφόρηση στο δίκτυο. Για παράδειγμα, σε ένα έξυπνο σπίτι, τα δεδομένα από συσκευές, όπως θερμοστάτες και συστήματα ασφαλείας, μπορούν να υποστούν επεξεργασία σε πραγματικό χρόνο, βελτιώνοντας την απόδοση και την εμπειρία του χρήστη [17], [5].

2.2.4.2. Αυτόνομη Οδήγηση

Η αυτόνομη οδήγηση απαιτεί την ανάλυση δεδομένων σε πραγματικό χρόνο για την ασφαλή λειτουργία των οχημάτων. Οι αισθητήρες των οχημάτων συλλέγουν δεδομένα σχετικά με την κίνηση, τα εμπόδια και τις συνθήκες του δρόμου. Το fog computing επιτρέπει την τοπική επεξεργασία αυτών των

δεδομένων σε κόμβους ομίχλης, οι οποίοι βρίσκονται σε πλησιέστερες υποδομές, όπως έξυπνες πινακίδες και φωτεινοί σηματοδότες. Με αυτόν τον τρόπο, εξασφαλίζεται η ταχύτερη απόκριση και μειώνεται η πιθανότητα ατυχημάτων λόγω καθυστερήσεων [17].

2.2.4.3. Βιομηχανική Αυτοματοποίηση

Στη βιομηχανία, το fog computing ενισχύει τα Συστήματα Ελέγχου Εποπτείας και Απόκτησης Δεδομένων (SCADA) που χρησιμοποιούνται για την παρακολούθηση και τον έλεγχο βιομηχανικών διεργασιών. Οι κόμβοι ομίχλης επιτρέπουν τη συλλογή, την επεξεργασία και την ανάλυση δεδομένων από αισθητήρες και συσκευές σε εργοστασιακούς χώρους σε πραγματικό χρόνο. Αυτό διευκολύνει την ταχύτερη λήψη αποφάσεων και τη μείωση των διακοπών λειτουργίας. Επιπλέον, η δυνατότητα αποθήκευσης δεδομένων τοπικά προσφέρει μεγαλύτερη ιδιωτικότητα και ασφάλεια [2].

2.2.4.4. Έξυπνα Δίκτυα Ενέργειας (Smart Grids)

Τα έξυπνα δίκτυα ενέργειας βασίζονται στο fog computing για την παρακολούθηση και τη διαχείριση της κατανάλωσης ενέργειας σε πραγματικό χρόνο. Οι κόμβοι ομίχλης, οι οποίοι βρίσκονται σε υποσταθμούς ή σε άλλες κρίσιμες θέσεις του δικτύου, επεξεργάζονται δεδομένα από μετρητές ενέργειας και αισθητήρες, επιτρέποντας τη βελτιστοποίηση της κατανομής ενέργειας. Αυτή η μέθοδος βοηθά στη μείωση της κατανάλωσης ενέργειας, στην αποτροπή υπερφόρτωσης του δικτύου και στην αποτελεσματική ενσωμάτωση ανανεώσιμων πηγών ενέργειας [17], [5].

2.2.4.5. Υγειονομική Περίθαλψη

Η υγειονομική περίθαλψη επωφελείται σε μεγάλο βαθμό από το fog computing, ιδίως στην απομακρυσμένη παρακολούθηση ασθενών μέσω συσκευών IoT. Οι συσκευές αυτές, όπως οι φορετές συσκευές (wearables), παρακολουθούν ζωτικά σημεία και άλλα κρίσιμα δεδομένα από τον ασθενή, τα οποία επεξεργάζονται τοπικά από κόμβους ομίχλης προτού αποσταλούν σε κεντρικά συστήματα για περαιτέρω ανάλυση. Οι κόμβοι ομίχλης σε τέτοια σενάρια τοποθετούνται συνήθως εντός των ιατρικών μονάδων (όπως νοσοκομεία και κλινικές), σε τοπικούς σταθμούς τηλεϊατρικής ή σε υποδομές του παρόχου υγείας κοντά στον χώρο του ασθενούς, ώστε η προεπεξεργασία να πραγματοποιείται όσο το δυνατόν πιο κοντά στην πηγή των δεδομένων. Σε περιβάλλοντα απομακρυσμένης φροντίδας, οι fog nodes μπορεί να βρίσκονται σε τοπικούς servers του εκάστοτε παρόχου ή σε αποκεντρωμένες μονάδες υγείας, επιτρέποντας άμεση ανάλυση και ανταπόκριση σε επείγοντα περιστατικά. Με αυτόν τον τρόπο, οι πάροχοι υγειονομικής περίθαλψης μπορούν να αντιδρούν γρήγορα σε καταστάσεις έκτακτης ανάγκης, ενώ παράλληλα διασφαλίζεται η ιδιωτικότητα των ασθενών [5].

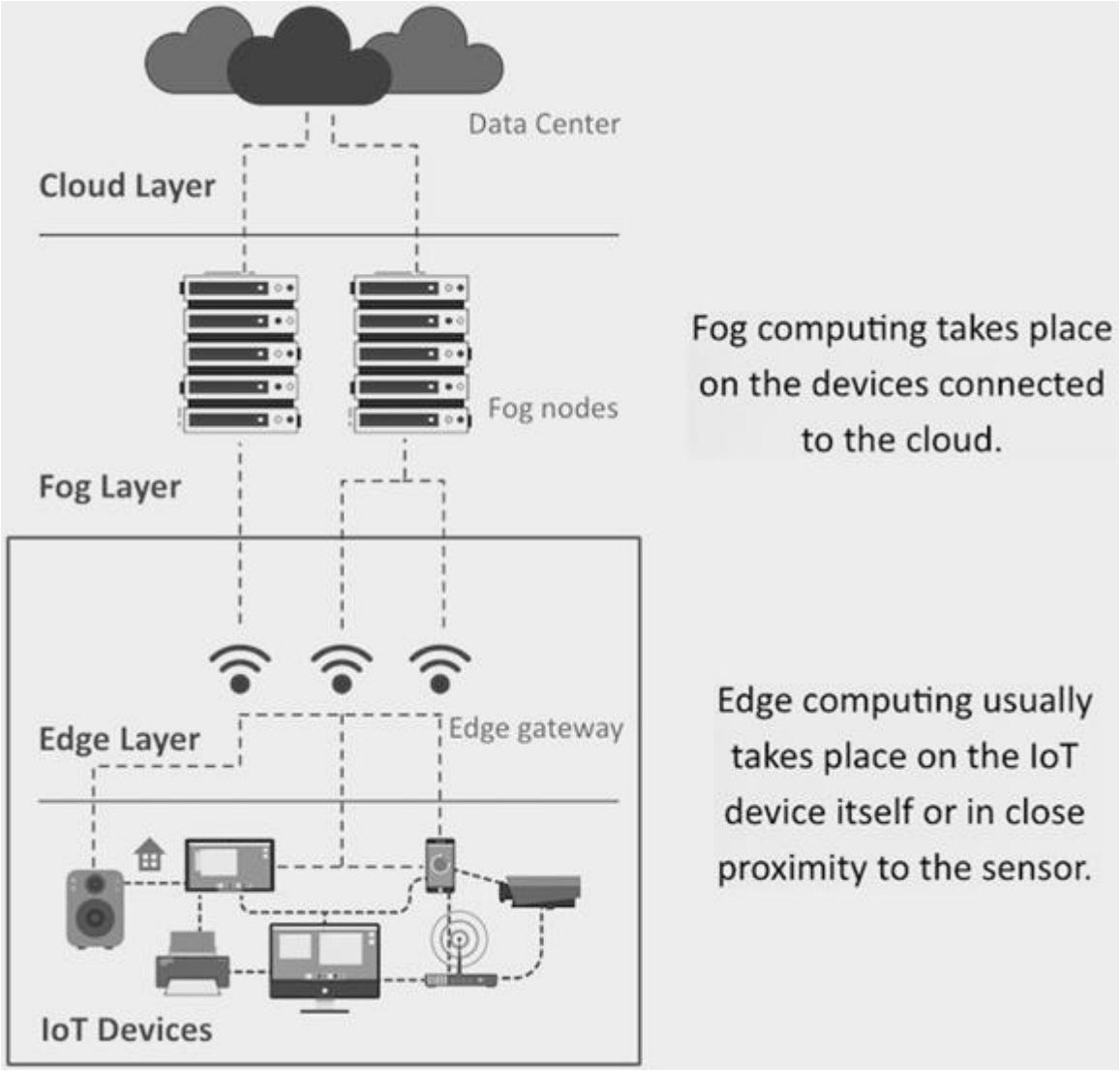
2.2.4.6. Έξυπνες Πόλεις

Οι έξυπνες πόλεις χρησιμοποιούν το fog computing για να ενισχύσουν την απόδοση διαφόρων υποδομών, όπως το σύστημα φωτεινών σηματοδοτών, τις

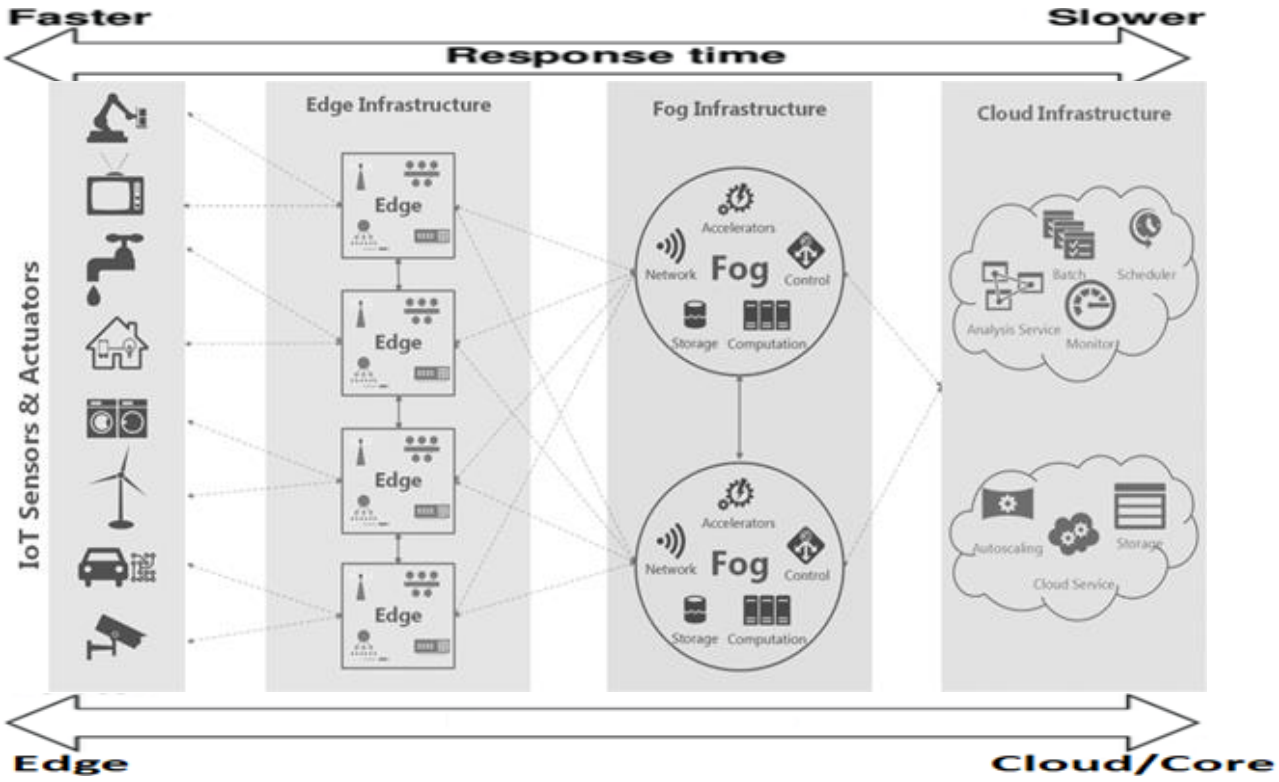
δημόσιες μεταφορές και τη διαχείριση αποβλήτων. Για παράδειγμα, οι κόμβοι ομίχλης βρίσκονται συνήθως σε τοπικούς σταθμούς κυκλοφοριακής διαχείρισης, σε roadside units (RSUs) που είναι εγκατεστημένα σε κόμβους οδικού δικτύου, σε smart intersections controllers, καθώς και σε δημοτικούς μικρο-εξυπηρετητές (city micro-data centers) που βρίσκονται κοντά στα σημεία συλλογής των δεδομένων. Οι κόμβοι αυτοί αναλύουν δεδομένα από αισθητήρες και κάμερες σε πραγματικό χρόνο, βελτιώνοντας τη ροή της κυκλοφορίας και μειώνοντας τη συμφόρηση, ενώ η τοπολογική τους εγγύτητα μειώνει δραστικά την καθυστέρηση σε κρίσιμες αποφάσεις [2], [5], [17].

Το fog computing έχει αναδειχθεί ως η ιδανική λύση για εφαρμογές που απαιτούν χαμηλή καθυστέρηση, υψηλή απόδοση και ενισχυμένη ασφάλεια. Από το IoT και την αυτόνομη οδήγηση έως τη βιομηχανία και τις έξυπνες πόλεις, η ευελιξία και οι δυνατότητές του το καθιστούν απαραίτητο εργαλείο για τις προκλήσεις του σύγχρονου κόσμου [2], [17], [5].

2.3 Τι είναι ο Υπολογισμός στις Ακμές του Δικτύου (Edge Computing)



Εικόνα 3: Αρχιτεκτονική του edge computing [14] [15] .



Εικόνα 4: Overall picture of cloud computing [16].

2.3.1 Ορισμός

Ο υπολογισμός στις ακμές του δικτύου (Edge Computing) αναφέρεται στη διαδικασία επεξεργασίας δεδομένων πλησίον της πηγής όπου παράγονται, αντί να μεταφέρονται σε κεντρικά κέντρα δεδομένων ή στο υπολογιστικό νέφος. Σε αντίθεση με το fog computing, το οποίο λειτουργεί ως ενδιάμεσο επίπεδο μεταξύ των συσκευών και του υπολογιστικού νέφους, το edge computing μεταφέρει την επεξεργασία όσο το δυνατόν πιο κοντά στην πηγή των δεδομένων, δηλαδή απευθείας στις ίδιες τις συσκευές ή σε άμεσα γειτονικούς πόρους τους. Επομένως, το fog computing συνήθως υλοποιείται μέσω ενδιάμεσων κόμβων (π.χ. gateways, routers ή μικροδιακομιστές σε τοπικά δίκτυα), ενώ το edge computing υλοποιείται σε επίπεδο τελικής συσκευής (της ίδιας που παράγει δεδομένα ή διπλανή της) ή σε edge servers που βρίσκονται δίπλα στις συσκευές. Με αυτόν τον τρόπο, το edge δίνει προτεραιότητα στην ελάχιστη δυνατή καθυστέρηση, ενώ το fog παρέχει ένα πιο οργανωμένο επίπεδο συντονισμού και διαχείρισης πόρων σε τοπική ή περιφερειακή κλίμακα (regional scale).

Η αρχιτεκτονική του Edge Computing αποσκοπεί στη μείωση της καθυστέρησης, στη βελτίωση της απόδοσης του δικτύου και στην παροχή άμεσων απαντήσεων σε πραγματικό χρόνο. Αυτή η λύση γίνεται ιδιαίτερα σημαντική σε εφαρμογές όπου η ταχύτητα είναι κρίσιμη, όπως η αυτόνομη οδήγηση και οι έξυπνες πόλεις [17], [5].

2.3.2 Χαρακτηριστικά και Πλεονεκτήματα του Edge Computing

2.3.2.1 Τοπική επεξεργασία

Το Edge Computing βασίζεται στην τοπική επεξεργασία δεδομένων, η οποία πραγματοποιείται πολλές φορές απευθείας στις συσκευές ή στους κόμβους που βρίσκονται στις ακμές του δικτύου (edge). Αυτές οι συσκευές, όπως αισθητήρες IoT, κάμερες, και άλλες έξυπνες συσκευές, είναι εξοπλισμένες με την απαραίτητη υπολογιστική ισχύ και μνήμη για την εκτέλεση τοπικών λειτουργιών επεξεργασίας. Στην πραγματικότητα, η δυνατότητα τοπικής επεξεργασίας επιτρέπει στα δεδομένα να αναλύονται στο σημείο παραγωγής τους, αποφεύγοντας την εξάρτηση από κεντρικές υποδομές υπολογιστικού νέφους, οι οποίες μπορεί να είναι γεωγραφικά απομακρυσμένες.

Κατα συνέπεια με αυτόν τον τρόπο το edge computing περιορίζει την ανάγκη για συνεχείς μεταφορές δεδομένων στο νέφος, καθώς η τοπική επεξεργασία επιτρέπει τη διαχείριση των περισσότερων πληροφοριών κοντά στην πηγή τους. Η άμεση ανάλυση των δεδομένων στο σημείο παραγωγής τους μειώνει σημαντικά τις καθυστερήσεις που σχετίζονται με τη μετάδοση και καθιστά εφικτή τη λήψη αποφάσεων σε πραγματικό χρόνο. Αυτό είναι ζωτικής σημασίας για εφαρμογές όπου η άμεση αντίδραση είναι απαραίτητη, όπως στην ανίχνευση ανωμαλιών σε βιομηχανικές εγκαταστάσεις. Για παράδειγμα, ένας αισθητήρας σε μια βιομηχανική μηχανή μπορεί να ανιχνεύσει άμεσα μια ανωμαλία και να ενεργοποιήσει ένα σύστημα ειδοποίησης ή να διακόψει τη λειτουργία της μηχανής, χωρίς να χρειάζεται να στείλει τα δεδομένα σε ένα απομακρυσμένο κέντρο δεδομένων [17], [8].

Παράλληλα, η επεξεργασία και το φιλτράρισμα των δεδομένων σε επίπεδο edge μειώνει το εύρος ζώνης που απαιτείται για τη μεταφορά δεδομένων, βελτιώνοντας τη συνολική απόδοση του δικτύου και περιορίζοντας τη συμφόρηση σε περιβάλλοντα με μεγάλο αριθμό συσκευών IoT που παράγουν συνεχώς πληροφορία [5].

2.3.2.2 Ιεραρχική αρχιτεκτονική και ενδιάμεσο επίπεδο επεξεργασίας

Εκτός από την επεξεργασία απευθείας στις edge συσκευές, το Edge Computing περιλαμβάνει και ένα ενδιάμεσο επίπεδο, αποτελούμενο από edge servers ή micro-edge nodes. Πρόκειται για μικρές υπολογιστικές μονάδες, τοποθετημένες τοπικά πιο κοντά από το νέφος αλλά υψηλότερα από τις IoT συσκευές, οι οποίες σχηματίζουν ιεραρχία 2–3 επιπέδων. Το ενδιάμεσο αυτό επίπεδο ενεργεί όταν οι IoT συσκευές δεν διαθέτουν επαρκή υπολογιστική ισχύ για την απαιτούμενη επεξεργασία.

Με αυτόν τον τρόπο, η επεξεργασία γίνεται σχεδόν τοπικά, χωρίς να απαιτείται μετάδοση δεδομένων προς το cloud, αποφεύγοντας έτσι καθυστερήσεις που μπορεί να είναι μη ανεκτές για εφαρμογές πραγματικού χρόνου. Η ιεραρχική δομή του edge computing ενισχύει την αξιοπιστία, καθώς οι edge servers μπορούν να αναλάβουν πιο απαιτητικές λειτουργίες από αυτές που μπορούν να εκτελέσουν οι συσκευές IoT, διατηρώντας παράλληλα την εγγύτητα των δεδομένων στο σημείο παραγωγής.

2.3.2.3 Υποστήριξη Εφαρμογών Πραγματικού Χρόνου

Η βασική αρχή που καθιστά το edge computing κατάλληλο για εφαρμογές πραγματικού χρόνου είναι η ικανότητά του να εκτελεί επεξεργασία δεδομένων απευθείας στην πηγή δημιουργίας τους, δηλαδή στις συσκευές ακμής ή σε πολύ κοντινούς κόμβους. Η επεξεργασία αυτή πραγματοποιείται τοπικά και άμεσα, χωρίς την ανάγκη αποστολής δεδομένων σε απομακρυσμένους εξυπηρετητές, γεγονός που μειώνει καθοριστικά τον συνολικό χρόνο απόκρισης του συστήματος [17].

Η τοπολογική εγγύτητα του επιπέδου ακμής (edge layer) προς τις πηγές δεδομένων οδηγεί σε δραστική μείωση της λανθάνουσας καθυστέρησης (latency) και εξαλείφει την εξάρτηση από την επίδοση του δικτύου μεταξύ χρήστη και cloud. Επιπλέον, η κατανομή του υπολογιστικού φορτίου σε πολλούς κόμβους αυξάνει την ανθεκτικότητα του συστήματος και συμβάλλει στη διατήρηση σταθερών χρόνων απόκρισης ακόμη και σε περιόδους αιχμής ή αποτυχίας μεμονωμένων κόμβων [5].

Το edge computing αξιοποιεί ελαφριά υπολογιστικά μοντέλα και αλγορίθμους βελτιστοποιημένους για λειτουργία σε περιβάλλοντα περιορισμένων πόρων. Οι συσκευές αυτές, αν και δεν διαθέτουν την ισχύ ενός cloud data center, είναι επαρκώς εξοπλισμένες ώστε να εκτελούν κρίσιμες ενέργειες σε πραγματικό χρόνο, όπως φιλτράρισμα, προ-επεξεργασία ή απλές μορφές ανάλυσης δεδομένων, αμέσως μετά τη λήψη των σημάτων.

Η υποστήριξη εφαρμογών πραγματικού χρόνου βασίζεται, επομένως, στην αποκέντρωση της υπολογιστικής ισχύος, στη μείωση της διαδρομής των δεδομένων, και στην άμεση πρόσβαση στους αισθητήρες και τους ενεργοποιητές, επιτρέποντας την ταχύτερη λήψη αποφάσεων και την εκτέλεση κρίσιμων εντολών χωρίς παρεμβολές [9].

2.3.2.4 Ιδιωτικότητα και Ασφάλεια

Η τοπική επεξεργασία δεδομένων που εφαρμόζεται από το Edge Computing μειώνει τους κινδύνους παραβίασης δεδομένων, καθώς τα δεδομένα δεν χρειάζεται να μεταφέρονται σε απομακρυσμένα κέντρα δεδομένων. Αυτό εξασφαλίζει την προστασία της ιδιωτικότητας, καθώς τα δεδομένα παραμένουν κοντά στην πηγή τους (ή και ακριβώς στην πηγή τους), μειώνοντας την έκθεση τους σε ενδεχόμενους κινδύνους κατά τη διάρκεια της μεταφοράς τους. Σε επίπεδο περιεχομένου, οι συσκευές ακμής αξιοποιούν συνήθως συμμετρική κρυπτογράφηση, όπως ο AES, για την προστασία των δεδομένων που αποθηκεύονται ή μεταφέρονται. Αντίθετα, ασύμμετροι αλγόριθμοι χρησιμοποιούνται κυρίως για ανταλλαγή κλειδιών και ψηφιακές υπογραφές (έλεγχος ακεραιότητας και αυθεντικότητας). Στα edge περιβάλλοντα, προτιμώνται ελαφρύτερες λύσεις, όπως η ελλειπτική καμπύλη (ECC), μέσω μηχανισμών όπως ECDH για ανταλλαγή κλειδιών και ECDSA για υπογραφές, ενώ ο RSA, θεωρείται πιο βαρύς υπολογιστικά και χρησιμοποιείται περιορισμένα. Ειδικά σε εφαρμογές όπου διακινούνται ευαίσθητες πληροφορίες, όπως σε συστήματα υγείας, τέτοιοι μηχανισμοί θεωρούνται απαραίτητοι για την πλήρη συμμόρφωση με κανονιστικά πλαίσια, όπως ο GDPR.

Επιπρόσθετα, είναι κρίσιμο να ενσωματώνονται μηχανισμοί αυθεντικοποίησης (authentication) και εξουσιοδότησης (authorization). Οι πρώτοι επιβεβαιώνουν την ταυτότητα κάθε συσκευής ή χρήστη που επιχειρεί να αποκτήσει πρόσβαση στο σύστημα, ενώ οι δεύτεροι καθορίζουν το επίπεδο πρόσβασης και τις ενέργειες που επιτρέπονται για κάθε οντότητα. Συνήθως, οι λειτουργίες αυτές υλοποιούνται μέσω token-based μηχανισμών (π.χ. OAuth 2.0, JWT) ή ενσωματώνονται στα πρωτόκολλα επικοινωνίας, όπως σε MQTT over TLS (IoT messaging με πιστοποίηση) και CoAP over DTLS (IoT lightweight πρωτόκολλο με ασφάλεια), όπου η ταυτοποίηση και η ασφαλής ανταλλαγή δεδομένων πραγματοποιούνται μέσω κρυπτογραφικών καναλιών και πιστοποιητικών.

Ιδιαίτερα σημαντικός μηχανισμός διασφάλισης ιδιωτικότητας είναι η ανωνυμοποίηση των δεδομένων, η οποία εφαρμόζεται ώστε να μην είναι δυνατή η ταυτοποίηση συγκεκριμένων χρηστών ή συσκευών βάσει των δεδομένων που παράγονται ή διακινούνται. Η τεχνική αυτή προσφέρει ένα επιπλέον επίπεδο προστασίας, καθώς καθιστά μη αναγνωρίσιμη την προέλευση των δεδομένων ακόμα και στην περίπτωση παραβίασης.

Συνολικά, η προστασία της ιδιωτικότητας και η ενίσχυση της ασφάλειας στο edge επιτυγχάνονται μέσω ενός πολυεπίπεδου πλαισίου μηχανισμών: από την κρυπτογραφημένη επικοινωνία και τα πρωτόκολλα ασφάλειας, μέχρι την αυθεντικοποίηση, την εξουσιοδότηση και την ανωνυμοποίηση των δεδομένων, όπου όλοι είναι κρίσιμοι για την ασφαλή αξιοποίηση του edge computing σε ευαίσθητες και δυναμικές εφαρμογές.

2.3.2.5 Ενεργειακή Αποδοτικότητα

Η ενεργειακή αποδοτικότητα είναι ένας από τους βασικούς λόγους υιοθέτησης του Edge Computing, ιδιαίτερα σε εφαρμογές όπου η συνεχής μετάδοση μεγάλου όγκου δεδομένων προς απομακρυσμένες υποδομές δεν είναι πρακτική. Η επεξεργασία δεδομένων τοπικά, κοντά στην πηγή δημιουργίας τους, επιτρέπει τη μείωση του όγκου πληροφοριών που απαιτείται να σταλεί προς το νέφος ή σε απομακρυσμένα κέντρα δεδομένων, γεγονός που περιορίζει σημαντικά τη συνολική κατανάλωση ενέργειας του συστήματος [17].

Η μεταφορά δεδομένων σε μεγάλες αποστάσεις ακόμη και αν αυτή γίνεται μέσω ενδιάμεσων κόμβων (π.χ. fog nodes ή gateways), συνεπάγεται ενεργοποίηση πολλαπλών διαδρομών στο δίκτυο, ενεργοποίηση μονάδων επικοινωνίας (π.χ. Wi-Fi, LTE) και χρήση πρωτοκόλλων μεταφοράς, τα οποία επιβαρύνουν ενεργειακά τόσο τις συσκευές όσο και την υποδομή [17]. Αντιθέτως, στο edge μοντέλο, η πρωτογενής επεξεργασία πραγματοποιείται στις ίδιες τις συσκευές ή σε κοντινούς edge κόμβους, μειώνοντας τον αριθμό μεταδόσεων και άρα την ενεργειακή επιβάρυνση.

Για την περαιτέρω ενίσχυση της αποδοτικότητας, πολλές συσκευές edge είναι εξοπλισμένες με χαμηλής κατανάλωσης επεξεργαστές και ενεργειακά ευφυείς λειτουργίες, όπως η αυτόματη μετάβαση σε κατάσταση αναμονής ("sleep mode") όταν δεν υπάρχει ενεργή επεξεργασία. Αυτός ο σχεδιασμός καθιστά το edge computing ιδιαίτερα κατάλληλο για περιβάλλοντα περιορισμένων πόρων,

όπως τα IoT, όπου η οικονομία ενέργειας είναι κρίσιμη για την αξιοπιστία και τη διάρκεια ζωής του συστήματος [5], [17].

Ωστόσο, θα πρέπει να σημειωθεί ότι η ενεργειακή αποδοτικότητα του edge δεν είναι αδιαμφισβήτητη σε κάθε περίπτωση. Δεδομένου ότι οι συσκευές edge έχουν περιορισμένη υπολογιστική ισχύ και μικρότερη ενεργειακή χωρητικότητα συγκριτικά με τις υποδομές ομίχλης, η ανάθεση έντονων εργασιών επεξεργασίας σε αυτές μπορεί, σε ορισμένα σενάρια, να επιφέρει υπερβολική κατανάλωση ενέργειας και μείωση της λειτουργικής τους απόδοσης. Αυτό είναι ιδιαίτερα σημαντικό όταν οι συσκευές αυτές επιτελούν πολλαπλές ταυτόχρονες λειτουργίες, γεγονός που αυξάνει τις απαιτήσεις τόσο σε υπολογιστική ισχύ όσο και σε ενέργεια.

Ως εκ τούτου, η ενεργειακή αποδοτικότητα στο edge computing πρέπει να αξιολογείται σε συνάρτηση με το φορτίο επεξεργασίας, τη διάρκεια λειτουργίας της συσκευής, και την κατανομή των υπολογιστικών εργασιών ανάμεσα στα επίπεδα της αρχιτεκτονικής (edge–fog–cloud). Σε επόμενη ενότητα σύγκρισης, θα αναδειχθούν αναλυτικά τα ενεργειακά trade-offs μεταξύ edge και fog, καθώς και οι επιπτώσεις τους στην ασφάλεια, τη διάρκεια ζωής συσκευών και την επιχειρησιακή απόδοση.

2.3.2.6 Μείωση Καθυστερήσεων

Το Edge Computing παρέχει τη δυνατότητα τοπικής επεξεργασίας δεδομένων, μειώνοντας δραστικά τον χρόνο απόκρισης. Αυτό είναι ιδιαίτερα σημαντικό σε εφαρμογές που απαιτούν λειτουργία σε πραγματικό χρόνο. Για παράδειγμα, στην αυτόνομη οδήγηση, οι αισθητήρες του οχήματος ανιχνεύουν εμπόδια και συλλέγουν δεδομένα για την κυκλοφορία και τις περιβαλλοντικές συνθήκες. Η τοπική επεξεργασία αυτών των δεδομένων στους κόμβους ακμής εξασφαλίζει ότι οι κρίσιμες αποφάσεις, όπως η αποφυγή εμποδίων ή η πέδηση, λαμβάνονται αμέσως, χωρίς τις καθυστερήσεις που θα προέκυπταν από τη μεταφορά τους στο νέφος. Παρομοίως, σε εφαρμογές υγειονομικής περίθαλψης, όπως η απομακρυσμένη παρακολούθηση ασθενών, οι τοπικοί κόμβοι μπορούν να ανιχνεύουν κρίσιμες αλλαγές στα ζωτικά όργανα/σημεία και να ειδοποιούν τους παρόχους υγείας άμεσα, αυξάνοντας την ταχύτητα ανταπόκρισης και μειώνοντας τους κινδύνους [17], [5].

2.3.2.7 Κλιμάκωση και Ευελιξία

Το edge computing παρουσιάζει σημαντικά πλεονεκτήματα ως προς την ευελιξία της αρχιτεκτονικής του και την ικανότητά του να προσαρμόζεται σε ένα ευρύ φάσμα εφαρμογών. Σε θεωρητικό επίπεδο, η δυνατότητα ενσωμάτωσης υπολογιστικών πόρων σε διαφορετικά σημεία του δικτύου επιτρέπει τη σταδιακή ανάπτυξη λύσεων χωρίς την ανάγκη για μαζικές και συγκεντρωτικές επενδύσεις σε υποδομές cloud [17]. Επιπλέον, η αποκεντρωμένη δομή του edge επιτρέπει την τοπική προσαρμογή των λειτουργιών, καθιστώντας το κατάλληλο για εφαρμογές με διαφορετικές απαιτήσεις, όπως σε περιβάλλοντα έξυπνων πόλεων ή βιομηχανικών εγκαταστάσεων [8].

Παρά τα παραπάνω, η ευελιξία αυτή συνοδεύεται από πρακτικές προκλήσεις που σχετίζονται με τα φυσικά όρια των συσκευών ακμής. Επειδή οι edge κόμβοι αποτελούνται συνήθως από αισθητήρες, μικροεπεξεργαστές ή άλλες υπολογιστικά περιορισμένες μονάδες, η δυνατότητά τους να υποστηρίξουν πολλαπλές, σύνθετες ή απαιτητικές λειτουργίες είναι περιορισμένη. Αυτό σημαίνει ότι η διαχείριση των πόρων τους απαιτεί προσεκτικό σχεδιασμό και συχνή παρακολούθηση της κατάστασης λειτουργίας τους (monitoring), ώστε να αποφεύγεται η υπερφόρτωση ή η αστοχία σε κρίσιμες συνθήκες [17].

Η ανάπτυξη εφαρμογών στο edge περιβάλλον δεν αφορά μόνο την τοποθέτηση περισσότερων συσκευών, αλλά και την ορθολογική κατανομή των φορτίων εργασίας, η οποία απαιτεί μηχανισμούς λήψης αποφάσεων σε πραγματικό χρόνο. Ειδικά σε περιπτώσεις όπου οι συσκευές είναι κινητές (π.χ. σε οχήματα, drones ή φορητές ιατρικές μονάδες), η κλιμάκωση γίνεται ακόμη πιο σύνθετη, καθώς απαιτείται η διατήρηση της συνδεσιμότητας και της ποιότητας υπηρεσίας (QoS) υπό μεταβαλλόμενες συνθήκες δικτύου.

Η απουσία ενός ενδιάμεσου επιπέδου (π.χ. fog) μπορεί να περιορίσει περαιτέρω τη λειτουργικότητα του edge μοντέλου, καθώς στερείται ενδιάμεσου σημείου ενοποίησης, προγραμματισμού και συντονισμού των τοπικών πόρων. Αυτό δημιουργεί την ανάγκη για εφαρμογή σύνθετων τεχνικών ελέγχου, προσαρμογής και πιθανώς αυτόματης μετανάστευσης εργασιών, ώστε να διατηρηθεί η επιχειρησιακή συνέχεια.

Συνολικά, ενώ η αρχιτεκτονική του edge computing χαρακτηρίζεται από υψηλή ευελιξία και δυνατότητα επέκτασης/κλιμάκωσης, η πρακτική υλοποίηση αυτών των χαρακτηριστικών εξαρτάται από την ύπαρξη μηχανισμών προηγμένης διαχείρισης πόρων, υποστήριξης κινητικότητας και έξυπνης παρακολούθησης. Η αξιολόγηση της κλιμάκωσης θα πρέπει επομένως να συνυπολογίζει τις τεχνικές και επιχειρησιακές προϋποθέσεις για την αποτελεσματική λειτουργία αυτών των συστημάτων, ιδιαίτερα σε περιβάλλοντα με έντονες μεταβολές φόρτου ή τοπολογίας.

2.3.2.8 Αύξηση Αξιοπιστίας και Υψηλή Διαθεσιμότητα

Η δυνατότητα των συστημάτων edge computing να παραμένουν λειτουργικά ανεξαρτήτως της κατάστασης διασύνδεσης με το νέφος προσδίδει σε αυτά υψηλό επίπεδο αξιοπιστίας και διαθεσιμότητας. Επειδή η επεξεργασία και ανάλυση των δεδομένων πραγματοποιείται τοπικά, μέσω των κόμβων ακμής, το σύστημα μπορεί να συνεχίσει να ανταποκρίνεται κανονικά ακόμη και σε περιπτώσεις προσωρινής διακοπής σύνδεσης με απομακρυσμένα κέντρα δεδομένων. Αυτή η αυτονομία είναι κρίσιμη σε εφαρμογές όπου η συνεχής λειτουργία είναι απαραίτητη, όπως στις βιομηχανικές εγκαταστάσεις, στην έξυπνη υγειονομική παρακολούθηση ή σε περιβάλλοντα απομακρυσμένης παρατήρησης [5].

Η τοπική αποθήκευση δεδομένων, σε συνδυασμό με την ικανότητα των κόμβων ακμής να εκτελούν κρίσιμες διεργασίες χωρίς εξωτερική εξάρτηση, ενισχύει τη συνολική ανθεκτικότητα του συστήματος σε αποτυχίες. Επιπλέον, σε

προηγμένα περιβάλλοντα edge, μπορούν να ενσωματωθούν μηχανισμοί ανίχνευσης σφαλμάτων (fault detection) και παρακολούθησης της «υγείας» των κόμβων. Οι μηχανισμοί αυτοί επιτρέπουν την προληπτική μετανάστευση φόρτου εργασίας από μία συσκευή σε άλλη, όταν ανιχνευθούν δείκτες υπερθέρμανσης, υπερφόρτωσης ή μείωσης της απόδοσης, διασφαλίζοντας έτσι τη συνέχιση της λειτουργίας χωρίς διακοπή.

Επιπρόσθετα, η αρχιτεκτονική edge μπορεί να ενσωματώσει τεχνικές υποστήριξης κινητικότητας, όπως δυναμική επανεκχώρηση ταυτοτήτων συσκευών, προσωρινή συγχώνευση με τοπικούς κόμβους πρόσβασης και caching δεδομένων, ώστε να εξασφαλίζεται η απρόσκοπτη λειτουργία ακόμη και σε συνθήκες φυσικής μετακίνησης των κόμβων (όπως σε οχήματα, drones ή φορητές ιατρικές μονάδες).

Συνεπώς, η αξιοπιστία στο edge computing δεν περιορίζεται μόνο στην τοπική αυτονομία, αλλά επεκτείνεται και στην ικανότητα του συστήματος να αντέχει σε σφάλματα, να αυτο-προσαρμόζεται σε δυναμικές συνθήκες λειτουργίας και να υποστηρίζει κινητικά σενάρια χωρίς απώλεια ποιότητας υπηρεσίας. Αυτά τα χαρακτηριστικά καθιστούν το edge computing κατάλληλο για εφαρμογές υψηλής διαθεσιμότητας, όπου η σταθερή λειτουργία είναι μη διαπραγματεύσιμη.

2.3.2.9 Εξοικονόμηση Πόρων

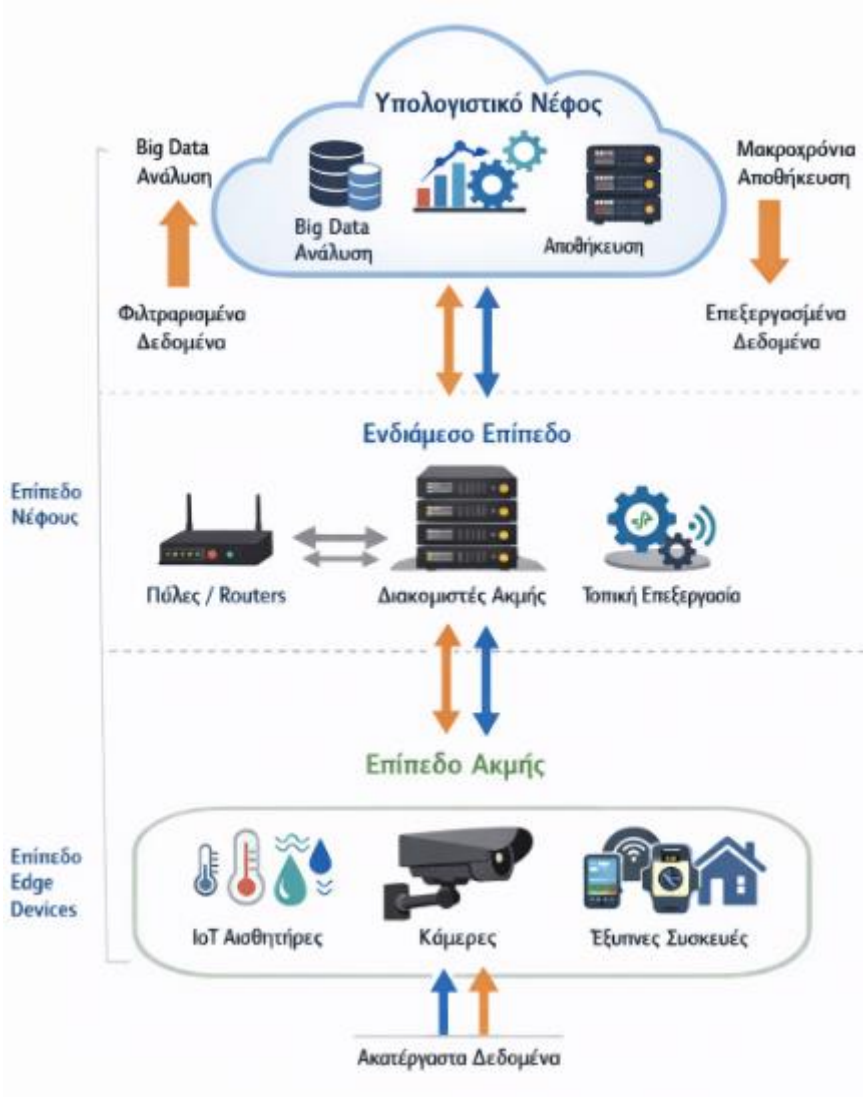
Η τοπική επεξεργασία δεδομένων στο edge computing επιτρέπει τον περιορισμό της ανάγκης αποστολής μεγάλων ποσοτήτων πληροφορίας προς απομακρυσμένα κέντρα δεδομένων, μειώνοντας έτσι σημαντικά τον φόρτο προς το υπολογιστικό νέφος. Ως αποτέλεσμα, περιορίζεται η κατανάλωση εύρους ζώνης προς εξωτερικές υποδομές, γεγονός που είναι κρίσιμο σε περιβάλλοντα με περιορισμένες δυνατότητες συνδεσιμότητας ή όπου η υπερφόρτωση του δικτύου μπορεί να επηρεάσει την απόδοση [17], [8]. Βεβαίως, η ανταλλαγή δεδομένων δεν εξαλείφεται πλήρως, καθώς εξακολουθεί να απαιτείται χρήση εύρους ζώνης σε τοπικό επίπεδο π.χ. μεταξύ κόμβων edge ή από κόμβους edge προς προς ενδιάμεσους edge servers / edge gateways, κάτι που ενδέχεται να δημιουργεί πιέσεις ανάλογα με την πυκνότητα του δικτύου και την κινητικότητα των συσκευών.

Η μείωση της εξάρτησης από το cloud συνεπάγεται επίσης μικρότερες απαιτήσεις για αποθήκευση και υπολογιστική ισχύ σε απομακρυσμένα data centers, οδηγώντας σε άμεση μείωση του σχετικού κόστους για τους οργανισμούς. Ωστόσο, αυτή η εξοικονόμηση δεν είναι απόλυτη: η τοπική επεξεργασία μεταφέρει μέρος του υπολογιστικού βάρους στις ίδιες τις συσκευές ακμής ή στους τοπικούς κόμβους edge, αυξάνοντας αντίστοιχα το κόστος απόκτησης, λειτουργίας και συντήρησης αυτών των συσκευών. Επομένως, παρατηρείται ένα χαρακτηριστικό trade-off ανάμεσα στην εξοικονόμηση πόρων από το cloud και την ανάγκη ενίσχυσης της τοπικής υποδομής [5], [17]. Σε αυτό το πλαίσιο, το edge computing είναι συχνά καταλληλότερο για οργανισμούς με περιορισμένους πόρους, καθώς επιτρέπει τη σταδιακή ανάπτυξη υποδομών σε μικρή κλίμακα, χωρίς να απαιτείται επένδυση σε μεγάλες και κεντρικά διαχειριζόμενες υποδομές.

Το ζήτημα γίνεται ακόμη πιο ενδιαφέρον αν εξεταστεί σε σχέση με το fog computing, όπου η ύπαρξη λιγότερων αλλά ισχυρότερων κόμβων συνεπάγεται διαφορετική προσέγγιση ως προς την απόδοση και την κατανομή του κόστους. Στο edge, η λογική προκρίνει την ύπαρξη περισσότερων, οικονομικότερων και λιγότερο ισχυρών κόμβων, γεγονός που επιτρέπει μεγαλύτερη ευελιξία, αλλά απαιτεί και πιο σύνθετους μηχανισμούς διαχείρισης και ελέγχου κατανομής φορτίου.

2.3.3 Αρχιτεκτονική του Edge Computing

Η αρχιτεκτονική του Edge Computing διαρθρώνεται σε τρία βασικά επίπεδα, τα οποία συνεργάζονται στενά για να παρέχουν αποδοτική διαχείριση δεδομένων, μειώνοντας την εξάρτηση από το κεντρικό νέφος. Κάθε επίπεδο παίζει συγκεκριμένο ρόλο στη συλλογή, την επεξεργασία και την αποθήκευση των δεδομένων.



Εικόνα 5: Η αρχιτεκτονική του edge computing

2.3.3.1 Επίπεδο Ακμής

Στη βάση της αρχιτεκτονικής βρίσκονται οι συσκευές ακμής, όπως αισθητήρες IoT, κάμερες, έξυπνοι μετρητές και άλλες συσκευές που συλλέγουν δεδομένα από το φυσικό περιβάλλον ή τους χρήστες. Αυτές οι συσκευές είναι εξοπλισμένες με βασικές δυνατότητες επεξεργασίας, επιτρέποντας το άμεσο φιλτράρισμα, τη μετατροπή ή τη συμπίεση των δεδομένων. Για παράδειγμα, ένας αισθητήρας IoT μπορεί να αναλύει δεδομένα θερμοκρασίας και να αποστέλλει μόνο κρίσιμα συμβάντα, μειώνοντας την περιττή μεταφορά δεδομένων προς τα ανώτερα επίπεδα.

Ανάλογα με τις δυνατότητές τους, ενδέχεται να εκτελούν πολύ βασική τοπική επεξεργασία, όπως απλό φιλτράρισμα (π.χ. thresholding, compression) ή προτυποποίηση σημάτων, αλλά σε πολλές περιπτώσεις περιορίζονται απλώς στη μετάδοση των ακατέργαστων δεδομένων προς το ενδιάμεσο επίπεδο.

Η επικοινωνία των συσκευών αυτών με τις πλησιέστερες μονάδες edge (στο ενδιάμεσο επίπεδο) βασίζεται κυρίως σε ασύρματα και ενεργειακά αποδοτικά πρωτόκολλα, όπως τα MQTT και CoAP, τα οποία μπορούν να ενσωματώνουν ελαφριά επίπεδα ασφάλειας (π.χ. DTLS αντί TLS) λόγω περιορισμένων υπολογιστικών πόρων [5], [17]. Η διασύνδεση μπορεί να υλοποιείται τόσο με ασύρματες τεχνολογίες (Wi-Fi, ZigBee, LoRaWAN) όσο και με ενσύρματες λύσεις (Ethernet, USB), ανάλογα με το περιβάλλον λειτουργίας και την κρισιμότητα της εφαρμογής.

Αυτή η τοπική επεξεργασία συμβάλλει στην εξοικονόμηση πόρων και στην ταχύτερη ανταπόκριση σε κρίσιμες εφαρμογές [17], [8].

2.3.3.2 Ενδιάμεσο Επίπεδο

Το ενδιάμεσο επίπεδο λειτουργεί ως γέφυρα μεταξύ των συσκευών ακμής και του υπολογιστικού νέφους και περιλαμβάνει μια συνδυαστική υποδομή που χωρίζεται σε δύο βασικές ομάδες: δικτυακές συσκευές και μονάδες επεξεργασίας. Οι πρώτες (όπως πύλες (gateways), διακομιστές ακμής (edge servers) και δρομολογητές (routers)) διαχειρίζονται την ασφαλή και αποδοτική διακίνηση των δεδομένων, επιτρέποντας την προσωρινή αποθήκευση και τη δρομολόγηση των ροών πληροφορίας. Μάλιστα, οι πύλες λειτουργούν ως συγκεντρωτές δεδομένων, συνδέοντας πολλαπλές συσκευές ακμής με το νέφος και ενισχύοντας την αποδοτικότητα του συστήματος.

Αντιθέτως, οι μονάδες επεξεργασίας (όπως μικροί edge servers ή gateways με ενσωματωμένους επεξεργαστές) αναλαμβάνουν το κύριο έργο ανάλυσης και προεπεξεργασίας των δεδομένων. Σε αυτό το επίπεδο, πραγματοποιείται τοπική ανάλυση δεδομένων, φιλτράρισμα, προσωρινή αποθήκευση και λήψη αποφάσεων σε πραγματικό χρόνο. Επιπλέον, το επίπεδο αυτό είναι υπεύθυνο για την προεπεξεργασία δεδομένων, διασφαλίζοντας ότι μόνο κρίσιμες πληροφορίες μεταφέρονται στα ανώτερα επίπεδα, μειώνοντας έτσι τον φόρτο του δικτύου και του νέφους [5]. Η μεταφορά δεδομένων από το ενδιάμεσο επίπεδο προς το cloud μπορεί να γίνεται με χρήση πρωτοκόλλων όπως HTTPS, AMQP, ή ακόμη και custom lightweight APIs μέσω REST ή gRPC [5], [17].

2.3.3.3 Επίπεδο Νέφους

Το επίπεδο του νέφους, μολονότι απομακρυσμένο από τις συσκευές ακμής, παραμένει κρίσιμο για τη συνολική αρχιτεκτονία. Οι υπηρεσίες cloud αναλαμβάνουν πολύπλοκες υπολογιστικές διεργασίες, αποθήκευση μεγάλης κλίμακας, ιστορική ανάλυση, καθώς και εκπαίδευση ή εκτέλεση μοντέλων μηχανικής μάθησης. Παρόλο που οι πόροι συγκεντρώνονται σε κεντρικές υποδομές, οι διαδικασίες μπορούν να υλοποιηθούν με κατανεμημένο τρόπο εντός του νέφους (π.χ. χρήση distributed computing frameworks όπως Apache Spark[11], Flink[12], ή Kubernetes[13]-based deployments).

Επιπλέον, το cloud μπορεί να αναλάβει την ενορχήστρωση edge-to-cloud ροών, αναλύοντας προεπεξεργασμένα ή επιλεγμένα δεδομένα που έχουν ήδη φιλτραριστεί τοπικά. Αυτή η συνεργατική προσέγγιση μειώνει την καθυστέρηση (latency), περιορίζει την κατανάλωση πόρων, και ενισχύει την ασφάλεια, αφού περιορίζεται η ανάγκη αποστολής ακατέργαστων δεδομένων [17].

Η συνολική αρχιτεκτονική του edge computing, επομένως, επιδιώκει να εκμεταλλευτεί τις δυνατότητες τοπικής επεξεργασίας, μειώνοντας την εξάρτηση από το cloud, χωρίς να το καταργεί, και να προσαρμόζεται σε διαφορετικά περιβάλλοντα χρήσης, από έξυπνες πόλεις και δίκτυα ενέργειας μέχρι βιομηχανικά και IoT οικοσυστήματα.

2.3.4 Εφαρμογές του Edge Computing

2.3.4.1 Διαδίκτυο των Πραγμάτων (IoT)

Το Edge Computing αποτελεί θεμελιώδη τεχνολογία για την υποστήριξη του Διαδικτύου των Πραγμάτων (IoT), καθώς δίνει τη δυνατότητα τοπικής επεξεργασίας δεδομένων κοντά στις πηγές που τα παράγουν. Για παράδειγμα, σε ένα έξυπνο σπίτι, οι συσκευές όπως θερμοστάτες, συστήματα φωτισμού και αισθητήρες κατανάλωσης ενέργειας μπορούν να επεξεργάζονται δεδομένα τοπικά, χωρίς να χρειάζεται να τα στέλνουν σε απομακρυσμένα κέντρα δεδομένων. Αυτή η τοπική ανάλυση επιτρέπει τη βελτιστοποίηση της ενεργειακής αποδοτικότητας, την αυτοματοποιημένη προσαρμογή συνθηκών, όπως η ρύθμιση θερμοκρασίας και φωτισμού, και την άμεση απόκριση σε αλλαγές του περιβάλλοντος. Επιπλέον, η μείωση της μεταφοράς δεδομένων ενισχύει την ασφάλεια και ιδιωτικότητα, ενώ μειώνει τον κίνδυνο καθυστερήσεων που θα μπορούσαν να επηρεάσουν την εμπειρία του χρήστη [17], [8].

2.3.4.2 Υγειονομική Περίθαλψη

Η υγειονομική περίθαλψη είναι ένας από τους τομείς όπου το Edge Computing έχει φέρει επανάσταση. Οι φορητές συσκευές (wearables), όπως έξυπνα

[11] Apache Spark — Unified analytics engine for large-scale data processing. Available at: https://spark.apache.org
[12] Apache Flink — Framework and distributed processing engine for stateful computations over data streams Available at: https://flink.apache.org
[13] Kubernetes — Open-source system for automating deployment, scaling, and management of containerized applications. Available at: https://kubernetes.io

ρολόγια και αισθητήρες παρακολούθησης καρδιακού ρυθμού ή πίεσης, συλλέγουν δεδομένα σε πραγματικό χρόνο. Αυτά τα δεδομένα αναλύονται τοπικά από τις ίδιες τις συσκευές ή από κοντινούς κόμβους ακμής, επιτρέποντας στους γιατρούς και τους παρόχους υγειονομικής περίθαλψης να λαμβάνουν κρίσιμες πληροφορίες άμεσα. Για παράδειγμα, μια φορητή συσκευή μπορεί να ανιχνεύσει μια επικίνδυνη αύξηση του καρδιακού ρυθμού και να ειδοποιήσει τόσο τον χρήστη όσο και τον γιατρό, εξοικονομώντας πολύτιμο χρόνο σε καταστάσεις έκτακτης ανάγκης. Επιπλέον, οι τοπικές επεξεργασίες μειώνουν την ανάγκη για μεταφορά ευαίσθητων δεδομένων στο νέφος, αυξάνοντας την ιδιωτικότητα των ασθενών [17], [5].

2.3.4.3 Βιομηχανική Αυτοματοποίηση

Στη βιομηχανία, το Edge Computing υποστηρίζει τη λειτουργία Συστημάτων Ελέγχου και Απόκτησης Δεδομένων (SCADA), τα οποία είναι υπεύθυνα για την παρακολούθηση και τον έλεγχο βιομηχανικών διεργασιών. Οι αισθητήρες που είναι ενσωματωμένοι σε βιομηχανικές μηχανές συλλέγουν δεδομένα, όπως θερμοκρασία, πίεση και δονήσεις, τα οποία επεξεργάζονται τοπικά στους κόμβους ακμής. Αυτή η διαδικασία μειώνει τις καθυστερήσεις και επιτρέπει την άμεση ανίχνευση προβλημάτων, όπως η αποτυχία ενός μηχανήματος. Οι τοπικές υποδομές ακμής εξασφαλίζουν επίσης τη συνεχή λειτουργία των συστημάτων, ακόμα και σε περιπτώσεις προσωρινής διακοπής της σύνδεσης με το νέφος, βελτιώνοντας έτσι τη συνολική απόδοση και την αξιοπιστία της βιομηχανικής παραγωγής [5].

2.3.4.4 Αυτόνομη Οδήγηση

Η αυτόνομη οδήγηση αποτελεί έναν από τους πιο απαιτητικούς τομείς για το Edge Computing, λόγω της ανάγκης για άμεσες αποφάσεις και επεξεργασία δεδομένων σε πραγματικό χρόνο. Τα οχήματα εξοπλισμένα με αισθητήρες, κάμερες και ραντάρ συλλέγουν τεράστιους όγκους δεδομένων από το περιβάλλον τους. Αυτά τα δεδομένα επεξεργάζονται τοπικά μέσω υποδομών ακμής, οι οποίες περιλαμβάνουν συσκευές που είναι ενσωματωμένες στο ίδιο το όχημα ή εντοπίζονται σε πλησιέστερες υποδομές, όπως έξυπνες πινακίδες ή φανάρια κυκλοφορίας. Αυτό επιτρέπει τη γρήγορη λήψη αποφάσεων, όπως η αποφυγή εμποδίων, η αλλαγή λωρίδας και η προσαρμογή της ταχύτητας σε πραγματικό χρόνο. Παράλληλα, η τοπική επεξεργασία μειώνει την εξάρτηση από την αποστολή δεδομένων στο νέφος, εξασφαλίζοντας την ασφάλεια και την ομαλή λειτουργία του οχήματος ακόμα και σε απομακρυσμένες περιοχές με περιορισμένη συνδεσιμότητα [9].

2.3.4.5 Έξυπνες Πόλεις

Το Edge Computing διαδραματίζει κεντρικό ρόλο στις έξυπνες πόλεις, υποστηρίζοντας υποδομές, όπως τα συστήματα διαχείρισης κυκλοφορίας, τα δίκτυα φωτισμού και τα συστήματα αποκομιδής απορριμμάτων. Για παράδειγμα, αισθητήρες τοποθετημένοι σε φανάρια κυκλοφορίας μπορούν να αναλύουν δεδομένα τοπικά για τη ροή της κυκλοφορίας και να προσαρμόζουν τη λειτουργία τους σε πραγματικό χρόνο, μειώνοντας τη συμφόρηση. Παρομοίως, έξυπνοι κάδοι απορριμμάτων με δυνατότητες

επεξεργασίας μπορούν να ειδοποιούν τις αρμόδιες υπηρεσίες όταν γεμίζουν, βελτιώνοντας την αποδοτικότητα των δρομολογίων αποκομιδής. Αυτή η τοπική επεξεργασία δεδομένων επιτρέπει την ταχύτερη λήψη αποφάσεων και βελτιώνει την ποιότητα ζωής των πολιτών [8].

Το Edge Computing, μέσα από την ευελιξία, την αποδοτικότητα και την αξιοπιστία του, καθιστά δυνατό τον εκσυγχρονισμό και τη βελτιστοποίηση διαδικασιών σε διάφορους τομείς. Από το IoT και τη βιομηχανία μέχρι τις έξυπνες πόλεις και την αυτόνομη οδήγηση, η τοπική επεξεργασία δεδομένων δημιουργεί νέες ευκαιρίες για καινοτομία και ανάπτυξη.

2.4 Συγκριτική Ανάλυση Fog και Edge Computing

Παρότι το fog computing και το edge computing συγκαταλέγονται στα σύγχρονα υπολογιστικά πρότυπα που στοχεύουν στη μείωση της καθυστέρησης και στην αποσυμφόρηση του υπολογιστικού νέφους, δεν αποτελούν ταυτόσημες έννοιες. Και τα δύο μοντέλα μεταφέρουν την επεξεργασία δεδομένων πιο κοντά στην πηγή παραγωγής τους, ωστόσο διαφέρουν ουσιαστικά ως προς το σημείο εκτέλεσης των υπολογισμών, τον τρόπο οργάνωσης των υποδομών, καθώς και τη λογική διαχείρισης και συντονισμού των πόρων. Η διάκριση μεταξύ των δύο είναι κρίσιμη, καθώς επηρεάζει τόσο την αρχιτεκτονική σχεδίαση ενός συστήματος όσο και την επιλογή της κατάλληλης τεχνολογίας ανάλογα με τις απαιτήσεις της εφαρμογής.

Όπως συνοψίζεται στον Πίνακα 2, το fog computing βασίζεται στη χρήση ενδιάμεσων κόμβων (fog nodes), οι οποίοι λειτουργούν ως κατανεμημένο στρώμα επεξεργασίας μεταξύ των συσκευών ακμής και του υπολογιστικού νέφους. Αντίθετα, το edge computing μεταφέρει την επεξεργασία όσο το δυνατόν πιο κοντά στην πηγή δεδομένων, δηλαδή απευθείας στις ίδιες τις συσκευές ή σε άμεσα γειτονικούς πόρους. Κατά συνέπεια, το edge δίνει προτεραιότητα στη μέγιστη δυνατή μείωση της καθυστέρησης, ενώ το fog παρέχει ένα πιο οργανωμένο επίπεδο συντονισμού και διαχείρισης πόρων σε τοπική ή περιφερειακή κλίμακα.

Πίνακας 2: Διαφορές Fog και Edge Computing

ΚΡΙΤΗΡΙΟ	FOG COMPUTING	EDGE COMPUTING
Θέση επεξεργασίας	Σε ενδιάμεσους κόμβους (gateways, edge servers)	Πάνω στις ίδιες τις IoT συσκευές ή πολύ κοντά σε αυτές
Απόσταση από την πηγή δεδομένων	Μικρή	Πολύ μικρή
Υπολογιστική ισχύς	Μέτρια έως υψηλή	Περιορισμένη
Καθυστέρηση (latency)	Πολύ μικρή	Ελάχιστη
Κλιμάκωση (scalability)	Υψηλότερη	Περιορισμένη
Κατανάλωση ενέργειας	Υψηλότερη από edge	Πολύ χαμηλή
Τυπικές εφαρμογές	Βιομηχανία, smart cities, aggregation IoT	Wearables, αισθητήρες, real-time ανίχνευση
Σχέση με Cloud	Ενδιάμεσο επίπεδο πριν το cloud	Άμεση ή μέσω fog

2.4.1 Θέση Επεξεργασίας και Αρχιτεκτονική Διαφοροποίηση

Η βασική διαφοροποίηση των δύο προτύπων αφορά το πού πραγματοποιείται η επεξεργασία. Στο edge computing, ο υπολογισμός ωθείται κατά προτεραιότητα στο τελικό επίπεδο, δηλαδή είτε πάνω στις ίδιες τις IoT συσκευές (π.χ. αισθητήρες, κάμερες, wearable devices) είτε σε edge servers, οι οποίοι είναι εγκατεστημένοι στο ίδιο φυσικό περιβάλλον ή στο ίδιο τοπικό δίκτυο. Ωστόσο, όταν η επεξεργασία δεν μπορεί να ολοκληρωθεί αποτελεσματικά στο τελικό επίπεδο, λόγω περιορισμών σε υπολογιστική ισχύ, μνήμη ή ενέργεια, προωθείται στο ενδιάμεσο επίπεδο (όπου και πάλι γίνονται εκμεταλλεύσιμοι edge servers εκτός και αν έχουμε μίξη των δύο μοντέλων οπότε μπορούν να χρησιμοποιηθούν και κόμβοι ομίχλης). Η προσέγγιση αυτή ελαχιστοποιεί τη χρονική καθυστέρηση και επιτρέπει την άμεση απόκριση σε συμβάντα.

Αντίθετα, στο fog computing, η επεξεργασία πραγματοποιείται εξαρχής στο ενδιάμεσο επίπεδο και όχι στο τελικό επίπεδο των συσκευών. Πιο συγκεκριμένα, ο υπολογισμός εκτελείται σε κόμβους με μεγαλύτερη υπολογιστική ισχύ σε σχέση με τις συσκευές edge, όπως IoT gateways, routers με υπολογιστικές δυνατότητες, micro-servers και μικρής κλίμακας τοπικά data centers. Οι κόμβοι αυτοί λειτουργούν ως περιφερειακό επίπεδο, το οποίο συγκεντρώνει δεδομένα από πολλαπλές συσκευές, εκτελεί προεπεξεργασία, συντονισμό και διαχείριση ροών δεδομένων πριν την αποστολή τους στο cloud.

2.4.2 Καθυστέρηση, Απόδοση και Διαχείριση Πόρων

Και τα δύο μοντέλα μειώνουν την καθυστέρηση σε σύγκριση με την αποκλειστική χρήση cloud computing, όμως το edge computing επιτυγχάνει συνήθως την ελάχιστη δυνατή καθυστέρηση, καθώς η επεξεργασία πραγματοποιείται πολλές φορές στο σημείο παραγωγής των δεδομένων. Αυτό το καθιστά ιδιαίτερα κατάλληλο για εφαρμογές όπου ακόμη και μικρές καθυστερήσεις είναι κρίσιμες, όπως η ανίχνευση ανωμαλιών σε βιομηχανικά συστήματα, η αυτόνομη οδήγηση ή η παρακολούθηση ασθενών σε πραγματικό χρόνο.

Το fog computing, από την άλλη, προσφέρει πλεονεκτήματα όταν απαιτείται συντονισμός πολλών edge συσκευών, διαχείριση μεγαλύτερου όγκου δεδομένων ή κατανομή φόρτου σε τοπικό επίπεδο. Λόγω της ύπαρξης fog nodes, το σύστημα μπορεί να αναλαμβάνει πιο απαιτητικές διεργασίες, όπως συγκεντρωτική ανάλυση δεδομένων, συνάθροιση (aggregation), caching και τοπική αποθήκευση, χωρίς να επιβαρύνει τις συσκευές ακμής.

2.4.3 Κλιμάκωση και Υποστήριξη Πολλαπλών Συσκευών

Το edge computing είναι ιδιαίτερα αποτελεσματικό όταν η επεξεργασία μπορεί να γίνει τοπικά ανά συσκευή ή ανά μικρό αριθμό συσκευών. Ωστόσο, η κλιμάκωσή του μπορεί να είναι πιο περιορισμένη, καθώς οι edge συσκευές διαθέτουν συχνά περιορισμένους πόρους (CPU, μνήμη, ενέργεια). Επομένως, η αύξηση του αριθμού συσκευών οδηγεί συχνά σε ανάγκη για πιο σύνθετη διαχείριση ή μεταφορά μέρους των εργασιών σε ανώτερα επίπεδα.

Αντίθετα, το fog computing είναι σχεδιασμένο ώστε να υποστηρίζει πιο αποδοτικά την κλιμάκωση σε περιβάλλοντα με μεγάλο αριθμό IoT συσκευών, καθώς οι fog nodes λειτουργούν ως ενδιάμεσοι συγκεντρωτικοί κόμβοι που μειώνουν την επιβάρυνση του cloud και οργανώνουν τη ροή δεδομένων σε περιφερειακή κλίμακα.

2.4.4 Σχέση με το Υπολογιστικό Νέφος

Η σχέση των δύο μοντέλων με το cloud διαφοροποιείται. Στο edge computing, η σύνδεση με το cloud μπορεί να είναι είτε άμεση είτε έμμεση μέσω ενδιάμεσων κόμβων (fog layer / edge gateways), με την αποστολή μόνο των πιο κρίσιμων ή συνοπτικών δεδομένων, ενώ μεγάλο μέρος της επεξεργασίας πραγματοποιείται τοπικά. Στο fog computing, το cloud παραμένει συνήθως το ανώτερο επίπεδο για μακροπρόθεσμη αποθήκευση, βαριά ανάλυση και κεντρική διαχείριση, αλλά η επικοινωνία οργανώνεται ιεραρχικά: τα δεδομένα αναχωρούν από το τερματικό επίπεδο (IoT/edge συσκευές), διέρχονται από ενδιάμεσες βαθμίδες κόμβων (π.χ. gateways, access/edge servers, micro-data

centers) όπου γίνεται συγκέντρωση/φιλτράρισμα/προεπεξεργασία, και στη συνέχεια προωθούνται προς το cloud.

2.4.5 Συνοπτική Σύγκριση Fog και Edge Computing

Συνοψίζοντας, το edge computing επικεντρώνεται στην άμεση επεξεργασία στο σημείο παραγωγής δεδομένων, επιτυγχάνοντας την ελάχιστη καθυστέρηση και περιορίζοντας τη μεταφορά πληροφορίας. Αντίθετα, το fog computing λειτουργεί ως ενδιάμεσο επίπεδο που επιτρέπει την καλύτερη οργάνωση πόρων, τον συντονισμό πολλών edge συσκευών και την αποδοτικότερη διαχείριση μεγάλων όγκων δεδομένων σε τοπική ή περιφερειακή κλίμακα. Επομένως, σε πολλές σύγχρονες αρχιτεκτονικές, τα δύο μοντέλα δεν λειτουργούν ανταγωνιστικά αλλά συμπληρωματικά, συνθέτοντας ένα πολυεπίπεδο σύστημα κατανεμημένης επεξεργασίας που γεφυρώνει τις δυνατότητες των IoT συσκευών με το υπολογιστικό νέφος.

3. Μεθοδολογία Ανασκόπησης

Η συστηματική διερεύνηση και τεκμηρίωση των θεμάτων που αφορούν την ασφάλεια και την ιδιωτικότητα στο fog computing και το edge computing, καθώς και η μελέτη του ρόλου της τεχνολογίας blockchain στη διαχείριση των προκλήσεων αυτών, απαιτεί την υιοθέτηση μιας αυστηρής συστηματικής βιβλιογραφικής μεθοδολογίας [19], [20] κατά την επιλογή της βιβλιογραφίας. Η μεθοδολογία της παρούσας συστηματικής βιβλιογραφικής ανασκόπησης διαμορφώθηκε με βάση τις καθιερωμένες κατευθυντήριες οδηγίες της Kitchenham για Systematic Literature Reviews (SLR) στον τομέα της πληροφορικής και της μηχανικής λογισμικού [19] [20]. Η εξασφάλιση ότι οι πηγές που χρησιμοποιούνται είναι έγκριτες, σύγχρονες και εστιασμένες στο αντικείμενο της μελέτης, αποτελεί προϋπόθεση για την αξιοπιστία και την εγκυρότητα των αποτελεσμάτων. Το παρών κεφάλαιο περιγράφει τα στάδια της διαδικασίας επιλογής βιβλιογραφίας, τα οποία περιλαμβάνουν: τη διαμόρφωση των ερευνητικών ερωτημάτων, την αναζήτηση επιστημονικών πηγών και την εφαρμογή κριτηρίων φιλτραρίσματος. Τέλος, παρέχεται μια ποσοτική ανάλυση των τελικών επιλογών ώστε να κατανοηθεί η κατανομή τους κατά μήκος διαφορετικών διαστάσεων.

3.1. Κύρια Ερευνητικά Ερωτήματα

Η διατύπωση σαφών και στοχευμένων ερευνητικών ερωτημάτων αποτελεί αναπόσπαστο στοιχείο κάθε επιστημονικής εργασίας. Η διερεύνηση των ζητημάτων ασφάλειας και ιδιωτικότητας στα fog και edge computing περιβάλλοντα, σε συνδυασμό με την αξιολόγηση της συνεισφοράς του blockchain στη θωράκιση των αρχιτεκτονικών αυτών, διαμόρφωσε τον πυρήνα των ερωτημάτων που τέθηκαν εξαρχής στο πλαίσιο της παρούσας μελέτης.

Τα βασικά ερωτήματα που καθοδήγησαν την αναζήτηση, επιλογή και ανάλυση της βιβλιογραφίας είναι τα εξής:

1. Ποια είναι τα κρίσιμα ζητήματα ασφάλειας και ιδιωτικότητας που εντοπίζονται στο fog computing και edge computing και πώς διαφοροποιούνται από αντίστοιχα ζητήματα σε πιο παραδοσιακές αρχιτεκτονικές, όπως το cloud computing;
2. Ποιοι είναι οι βασικοί κίνδυνοι και οι τεχνικές προκλήσεις αναφορικά με την προστασία της ιδιωτικής ζωής (δηλ. την ιδιωτικότητα) σε fog και edge computing περιβάλλοντα;
3. Ποιες λύσεις υπάρχουν για την αντιμετώπιση των ζητημάτων ασφάλειας & ιδιωτικότητας σε περιβάλλοντα fog & edge computing;
4. Πώς μπορεί η τεχνολογία blockchain να συνεισφέρει στην αντιμετώπιση αυτών των ζητημάτων σε fog και edge συστήματα;
5. Ποιοι είναι οι περιορισμοί και οι προκλήσεις της ενσωμάτωσης του blockchain στα περιβάλλοντα αυτά, ιδίως όσον αφορά την υπολογιστική απόδοση, την κατανάλωση ενέργειας και την επεκτασιμότητα/κλιμακωσιμότητα σε δυναμικά δίκτυα;
6. Πώς μπορούν συμπληρωματικές τεχνολογίες και αναδυόμενες ερευνητικές κατευθύνσεις, όπως η ενσωμάτωση τεχνητής νοημοσύνης

(AI) και μηχανικής μάθησης (ML), ως προς το blockchain, να βελτιώσουν περαιτέρω την ασφάλεια και την αποδοτικότητα αυτών των fog & edge συστημάτων;

Η κάλυψη των ανωτέρω ερωτημάτων παρέχεται & αναλύεται στα εξής μέρη της διπλωματικής:

Πίνακας 3: Ερωτήματα ανά κεφάλαιο

Ερευνητικό Ερώτημα	**Σχετικό Κεφάλαιο**
(1) Ζητήματα ασφάλειας & ιδιωτικότητας στο fog	Κεφάλαιο **4**
(2) Ζητήματα ασφάλειας & ιδιωτικότητας στο edge	Κεφάλαιο **4**
(3) Λύσεις ζητημάτων ασφάλειας & ιδιωτικότητας σε περιβάλλοντα fog & edge computing	Κεφάλαιο **4.3**
(4) Συνεισφορά blockchain στην αντιμετώπιση των ζητημάτων ασφάλειας & ιδιωτικότητας	Κεφάλαιο **5**
(5) Περιορισμοί & προκλήσεις ενσωμάτωσης blockchain	Κεφάλαιο **6**
(6) Ενσωμάτωση AI/ML και νέες ερευνητικές κατευθύνσεις	Κεφάλαιο **6**

Η παρούσα ενότητα λειτουργεί ως πλαισίωση για την κατανόηση των αναλύσεων που ακολουθούν, ενισχύοντας τη **θεματική συνοχή** και τη **λογική αλληλουχία** της εργασίας.

3.2. Πηγές & Τρόποι Αναζήτησης Άρθρων

Η διαδικασία συλλογής και αξιολόγησης της επιστημονικής βιβλιογραφίας στηρίχθηκε στη χρήση αναγνωρισμένων και έγκυρων ψηφιακών βάσεων δεδομένων, οι οποίες εξειδικεύονται στη διάθεση επιστημονικών άρθρων και ερευνητικών μελετών στον τομέα της πληροφορικής και των τεχνολογιών επικοινωνιών. Η επιλογή των συγκεκριμένων πηγών υπαγορεύτηκε από την ανάγκη διασφάλισης της αξιοπιστίας των πληροφοριών, την πρόσβαση σε πρόσφατες εξελίξεις και την ευρεία κάλυψη των αντικειμένων που σχετίζονται με το fog computing, το edge computing και την τεχνολογία blockchain.

Ειδικότερα, χρησιμοποιήθηκαν οι ακόλουθες βάσεις δεδομένων και ερευνητικές πλατφόρμες:

- *Google Scholar*: Αποτελεί μία από τις πλέον διαδεδομένες μηχανές αναζήτησης ακαδημαϊκού περιεχομένου, επιτρέποντας την πρόσβαση σε δημοσιεύσεις που καλύπτουν ένα ευρύ φάσμα επιστημονικών κλάδων. Η επιλογή της συγκεκριμένης πλατφόρμας στηρίχθηκε στη δυνατότητα συγκέντρωσης άρθρων από ποικίλες πηγές, συμπεριλαμβανομένων συνεδρίων, περιοδικών, πανεπιστημιακών εκδόσεων και τεχνικών αναφορών.
  Η συμπερίληψη πανεπιστημιακών εκδόσεων και τεχνικών αναφορών κρίθηκε σκόπιμη, καθώς σε τομείς όπως το fog/edge computing και το blockchain μεγάλο μέρος της τεχνολογικής εξέλιξης και των αρχιτεκτονικών προσεγγίσεων παρουσιάζεται αρχικά σε τεχνικά κείμενα, white papers και reports από ερευνητικούς οργανισμούς ή βιομηχανικούς φορείς, πριν δημοσιευθεί σε περιοδικά. Ωστόσο, τέτοιες πηγές χρησιμοποιήθηκαν επικουρικά και μόνο όταν πληρούσαν βασικά κριτήρια αξιοπιστίας (π.χ. σαφής προέλευση, τεκμηρίωση και επιστημονική συνάφεια).
- *IEEE Xplore*: Αποτελεί εξειδικευμένη βάση δεδομένων που εστιάζει στην επιστήμη των υπολογιστών, τα τηλεπικοινωνιακά δίκτυα και τα συστήματα πληροφορικής. Η χρήση της ήταν απαραίτητη για την εξασφάλιση πρόσβασης σε άρθρα υψηλής επιστημονικής αξίας, που προέρχονται από διακεκριμένα συνέδρια και περιοδικά του Ινστιτούτου Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE), οργανισμού με διεθνώς αναγνωρισμένο κύρος.
- *SpringerLink*: Η βάση δεδομένων της εκδοτικής εταιρείας Springer προσφέρει επιστημονικές δημοσιεύσεις που καλύπτουν πληθώρα γνωστικών αντικειμένων, μεταξύ των οποίων και η πληροφορική. Η επιλογή της συγκεκριμένης πλατφόρμας συνδέεται με την αξιοπιστία των εκδόσεών της και την ενσωμάτωση άρθρων που προέρχονται από έγκριτα περιοδικά και διεθνή συνέδρια που ανήκουν στην προαναφερόμενη εκδοτική εταιρεία.
- *ACM Digital Library*: Πρόκειται για την ψηφιακή βιβλιοθήκη της Ένωσης Υπολογιστικών Μηχανών (Association for Computing Machinery – ACM), η οποία αποτελεί σημαντική πηγή έρευνας στους τομείς της πληροφορικής και των δικτύων. Η χρήση της κρίθηκε αναγκαία λόγω της εστίασής της σε ζητήματα αιχμής που σχετίζονται με τις υπολογιστικές αρχιτεκτονικές, τα κατανεμημένα συστήματα και τις αναδυόμενες τεχνολογίες, όπως το fog και το edge computing.
- *MDPI*: Open-access επιστημονικός εκδοτικός οίκος με ενεργό ρόλο σε blockchain και fog computing θεματολογία.
- *arXiv.org*: Εκδόσεις άρθρων τύπου preprint (προ-δημοσίευσης) στους τομείς πληροφορικής, AI, ασφάλειας και συστημάτων. Οι πηγές αυτές, εφόσον τελικά δεν δημοσιεύθηκαν, χρησιμοποιήθηκαν επικουρικά και μόνο εφόσον πληρούσαν βασικά κριτήρια αξιοπιστίας (π.χ. σαφής προέλευση, τεκμηρίωση και επιστημονική συνάφεια).
- *ResearchGate.net, Academia.edu, Semantic Scholar (AI-enhanced)*: Δίκτυα ακαδημαϊκής δημοσίευσης με πλήρη πρόσβαση σε μεγάλο

αριθμό peer-reviewed άρθρων που παρέχεται από τους ίδιους τους συγγραφείς.

Η αναζήτηση άρθρων πραγματοποιήθηκε μέσω της χρήσης συγκεκριμένων λέξεων-κλειδιών και λογικών συνδυασμών αυτών, με σκοπό τον εντοπισμό δημοσιεύσεων που ανταποκρίνονται στο γνωστικό αντικείμενο της παρούσας διπλωματικής εργασίας. Ενδεικτικά, χρησιμοποιήθηκαν όροι όπως:

A. Πεδίο/Τεχνολογία

(("blockchain" | "distributed ledger" | DLT) & ("fog computing" | "edge computing" | "MEC" | "IoT"))

B. Ιδιότητα/Θέμα

("security" | "privacy" | "trust" | "authentication" | "access control")

C. Τύπος Εξέτασης

("challenges" | "limitations" | "constraints" | "solutions" | "mitigation" | "research directions" | "survey" **|** "study")

D. Συνολικό Template

(("blockchain" | "distributed ledger" | "DLT") & ("fog computing" | "edge computing" | "MEC" | "IoT")) & ("security" | "privacy" | "trust" | "authentication" | "access control") & ("challenges" | "limitations" | "constraints" | "solutions" | "mitigation" | "research directions" | "survey" **|** "study")

Χρησιμοποιήθηκαν επιπλέον χρονικά φίλτρα (2016–2025), ώστε να διασφαλιστεί η επικαιρότητα των ερευνών. Επιπλέον, εφαρμόστηκε έλεγχος διαθεσιμότητας πλήρους κειμένου σε μορφή PDF ως πρακτικό κριτήριο ανάκτησης και όχι ως αυστηρό κριτήριο αποκλεισμού. Συγκεκριμένα, όταν ένα άρθρο δεν ήταν άμεσα διαθέσιμο ως open-access, εξετάστηκε η δυνατότητα πρόσβασης μέσω ιδρυματικών συνδρομών (π.χ. πανεπιστημιακής βιβλιοθήκης), εναλλακτικά μέσω preprints/τεχνικών αναφορών (όπου υπήρχαν), ή μέσω επικοινωνίας με τους συγγραφείς. Μόνο εφόσον δεν κατέστη

δυνατή η απόκτηση πλήρους κειμένου με κανέναν από τους παραπάνω τρόπους, το άρθρο αποκλειόταν από τα τελικά στάδια της αξιολόγησης. Με αυτόν τον τρόπο περιορίζεται ο κίνδυνος να αποκλειστεί σημαντικό μέρος της σχετικής βιβλιογραφίας λόγω περιορισμών πρόσβασης.

Η επιλογή αυτών των συγκεκριμένων βάσεων δεδομένων και μεθόδων αναζήτησης κρίθηκε απαραίτητη, καθώς ανταποκρίνεται στις απαιτήσεις μιας ακαδημαϊκής εργασίας που επικεντρώνεται σε τεχνολογίες αιχμής, οι οποίες εξελίσσονται ραγδαία και απαιτούν πρόσβαση σε πρωτογενή επιστημονικά δεδομένα και έρευνες. Η αξιοποίηση των παραπάνω πλατφορμών κατέστησε δυνατή τη συγκέντρωση άρθρων δυνητικά υψηλής επιστημονικής αξίας, που προέρχονται από έγκριτους εκδοτικούς φορείς, εξασφαλίζοντας έτσι την εγκυρότητα των πηγών που αποτέλεσαν τη βάση της περαιτέρω ανάλυσης.

3.3. Φιλτράρισμα Άρθρων

Η διαδικασία φιλτραρίσματος και επιλογής της επιστημονικής βιβλιογραφίας αποτελεί αναπόσπαστο και καθοριστικό στάδιο κατά τη διαμόρφωση του θεωρητικού πλαισίου μιας διπλωματικής εργασίας. Στο πλαίσιο της παρούσας έρευνας, υιοθετήθηκε μια μεθοδική προσέγγιση αξιολόγησης των άρθρων που εντοπίστηκαν μέσω των ηλεκτρονικών βάσεων δεδομένων, με στόχο την επίτευξη υψηλής ποιότητας και αξιοπιστίας του τελικού συνόλου των πηγών. Η εφαρμογή συγκεκριμένων κριτηρίων αποδοχής, απόρριψης και ποιότητας αποτέλεσε τον βασικό άξονα του φιλτραρίσματος, ώστε να διασφαλιστεί ότι το τελικό σώμα βιβλιογραφίας ανταποκρίνεται στις απαιτήσεις της επιστημονικής εγκυρότητας και της θεματικής συνάφειας.

Ως προς τα κριτήρια αποδοχής/αποκλεισμού, λήφθηκαν υπόψη:

- **Η γλώσσα συγγραφής**: Έγιναν δεκτά μόνο άρθρα γραμμένα στην αγγλική γλώσσα καθώς η αγγλική αποτελεί την κυρίαρχη γλώσσα επιστημονικής διάχυσης στον χώρο της πληροφορικής, εξασφαλίζοντας πρόσβαση στο μεγαλύτερο μέρος της έγκριτης και συγκρίσιμης βιβλιογραφίας.
- **Η περίοδος δημοσίευσης**: Επιλέχθηκαν μόνο εργασίες που δημοσιεύθηκαν από το 2016 έως το 2025, προκειμένου να διασφαλιστεί η τεχνική και ερευνητική επικαιρότητα.
- **Διαθεσιμότητα πλήρους κειμένου**: Συμπεριλήφθηκαν μόνο άρθρα για τα οποία υπήρχε πλήρης πρόσβαση (είτε λόγω της ανοικτής μορφής τους είτε λόγω πρόσβασης μέσω του ιδρυματικού λογαριασμού του συγγραφέως), ώστε να είναι δυνατή η πλήρης αξιολόγηση της μεθοδολογίας και των αποτελεσμάτων.
- **Είδος δημοσίευσης**: Έγιναν δεκτές κατά κύριο λόγο εργασίες που έχουν υποβληθεί σε διαδικασία επιστημονικής αξιολόγησης (peer-review), όπως άρθρα σε επιστημονικά περιοδικά και δημοσιεύσεις σε πρακτικά συνεδρίων. Επιπλέον, συμπεριλήφθηκαν επιλεκτικά τεχνικές αναφορές (technical reports), κεφάλαια βιβλίων (book chapters), τεκμηρίωση πλατφορμών (platform documentation) blockchain καθώς και ακαδημαϊκές διατριβές (PhD theses/dissertations), μόνο όταν παρείχαν σαφή μεθοδολογία, τεχνική τεκμηρίωση και πρωτογενή

συνεισφορά σχετική με τα ερευνητικά ερωτήματα της εργασίας. Τα τελευταία ελέγχθηκαν μέσω των κριτηρίων ποιότητας που αναλύονται παρακάτω.

- **Θεματική συνάφεια (scope)**: Συμπεριλήφθηκαν μόνο εργασίες που αφορούν fog computing ή/και edge computing και εξετάζουν ζητήματα ασφάλειας/ιδιωτικότητας ή/και προσεγγίσεις αξιοποίησης του blockchain για την αντιμετώπιση αυτών των ζητημάτων. Σημειώνεται πως το κριτήριο αυτό είναι διττής φύσης (ένταξης & ποιότητας) διότι απαιτεί τον έλεγχό του τόσο στα μεταδεδομένα όσο και στο κυρίως περιεχόμενο μιας πηγής.

Ως προς τα κριτήρια ποιότητας, προτιμήθηκαν και ενσωματώθηκαν στην τελική ανάλυση μόνο εργασίες που πληρούσαν τα ακόλουθα:

- **Η μορφολογική και επιστημονική πληρότητα**: Λήφθηκε υπόψη η μορφολογική αρτιότητα των άρθρων, όπως η ύπαρξη δομημένης μεθοδολογίας, ανάλυσης, πειραμάτων (όπου εφαρμόζεται) και συμπερασμάτων, ώστε οι πηγές να είναι αξιοποιήσιμες για συστηματική ανάλυση.
- **Μεθοδολογική σαφήνεια και τεκμηρίωση**: Οι εργασίες έπρεπε να περιγράφουν με σαφήνεια τη μεθοδολογία, τα στάδια ανάλυσης και (όπου εφαρμόζεται) τα πειράματα ή την αξιολόγηση, ώστε να είναι δυνατή η κατανόηση και τελική διαλογή τους από τον συγγραφέα.
- **Θεματική συνάφεια με τα ερευνητικά ερωτήματα**: Οι πηγές έπρεπε να μπορούν να αξιοποιηθούν άμεσα για την απάντηση των ερευνητικών ερωτημάτων της παρούσας εργασίας, είτε μέσω ανάλυσης προκλήσεων είτε μέσω προτεινόμενων αρχιτεκτονικών/προσεγγίσεων. Επιπλέον, θα έπρεπε να είναι απόλυτα συναφείς με το αντικείμενο της μελέτης.
- **Υποστηρικτικό υλικό (διαγράμματα και παραδείγματα):** Θεωρήθηκε θετικό στοιχείο η ύπαρξη διαγραμμάτων, πινάκων ή παραδειγμάτων, καθώς διευκολύνουν την κατανόηση και την εξαγωγή συγκρίσιμων συμπερασμάτων.

Η συνολική διαδικασία φιλτραρίσματος είχε στόχο όχι μόνο τον περιορισμό του όγκου της βιβλιογραφίας, αλλά και τη διασφάλιση της θεματικής συνοχής, της επιστημονικής αρτιότητας και της αξιοποιήσιμης γνώσης που μπορούσε να εξαχθεί για την υποστήριξη των αναλύσεων στα επόμενα κεφάλαια της παρούσας εργασίας. Η διαδικασία πραγματοποιήθηκε σε δύο διακριτές φάσεις: (α) αρχικό φιλτράρισμα με βάση τα κριτήρια αποδοχής/αποκλεισμού, τα οποία αξιολογήθηκαν μέσω των μεταδεδομένων κάθε δημοσίευσης (π.χ. τίτλος, περίληψη, έτος, τύπος δημοσίευσης, διαθεσιμότητα πλήρους κειμένου), και (β) τελικό φιλτράρισμα με βάση τα κριτήρια ποιότητας, τα οποία αξιολογήθηκαν μέσω της ανάγνωσης και ανάλυσης του πλήρους περιεχομένου των επιλεγμένων εργασιών.

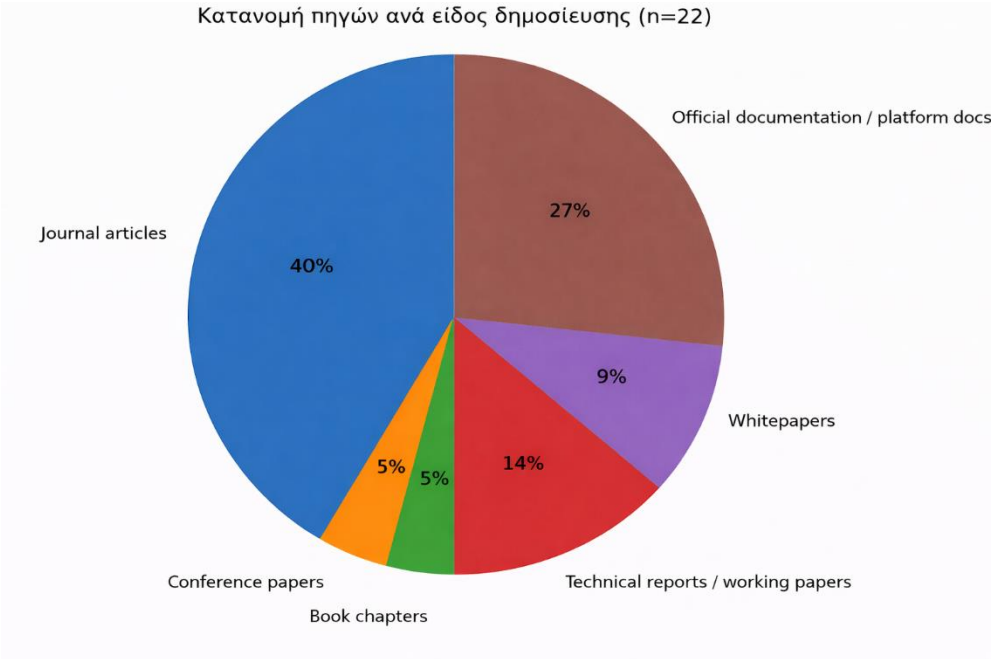
3.4. Στατιστική Επισκόπηση της Διαδικασίας Επιλογής Βιβλιογραφίας

Η διαδικασία συλλογής και φιλτραρίσματος της βιβλιογραφίας πραγματοποιήθηκε σε τρεις διακριτές φάσεις: (α) συλλογή βιβλιογραφίας μέσω αναζήτησης στις πηγές που αναφέρθηκαν στην Ενότητα 3.2, (β) αρχικό φιλτράρισμα συλλεγμένης βιβλιογραφίας με βάση τα κριτήρια αποδοχής/αποκλεισμού μέσω μεταδεδομένων (metadata filtering) και (γ) τελικό φιλτράρισμα με βάση τα κριτήρια ποιότητας μέσω αξιολόγησης πλήρους κειμένου (full-text filtering).

Συνολικά, συλλέχθηκαν αρχικά 200 εργασίες από τις επιλεγμένες επιστημονικές βάσεις δεδομένων και πλατφόρμες. Μετά την εφαρμογή των κριτηρίων αποδοχής/αποκλεισμού, διατηρήθηκαν 45 εργασίες. Τέλος, έπειτα από αξιολόγηση ποιότητας και ανάλυση πλήρους περιεχομένου, επιλέχθηκαν για την τελική ανασκόπηση 22 εργασίες. Η τελική διατήρηση 22 από τις 200 εργασίες (δηλαδή φιλτράρισμα 89%) είναι ενδεικτική μιας αυστηρής και καλά δομημένης διαδικασίας επιλογής, καθώς μεγάλο μέρος της αρχικής “ακατέργαστης” βιβλιογραφίας απορρίφθηκε συστηματικά ως μη επαρκώς συναφές, μη τεκμηριωμένο ή μη κατάλληλο για τα ερευνητικά ερωτήματα.

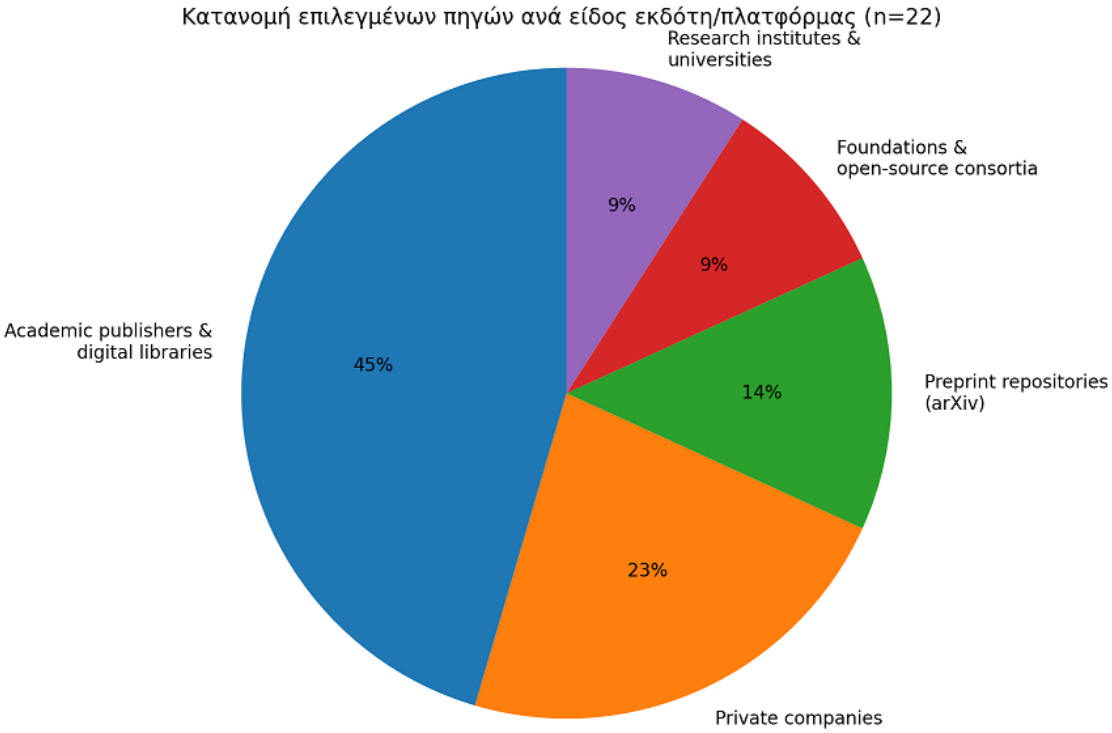
Στην παρούσα συστηματική ανασκόπηση δόθηκε προτεραιότητα σε peer-reviewed επιστημονικές δημοσιεύσεις (journal και conference papers). Παράλληλα, συμπεριλήφθηκε και επιλεγμένη “γκρίζα” βιβλιογραφία (grey literature) — όπως τεχνικές αναφορές/working papers και κεφάλαια βιβλίων — μόνο όταν (i) προέρχεται από αξιόπιστους φορείς (π.χ. ακαδημαϊκούς εκδότες, αναγνωρισμένους οργανισμούς/ιδρύματα), (ii) παρέχει πρωτογενή τεχνική τεκμηρίωση που δεν καλύπτεται επαρκώς από peer-reviewed άρθρα (π.χ. επίσημη αρχιτεκτονική/πρωτόκολλα), και (iii) αξιολογείται με τα ίδια κριτήρια ποιότητας (τεκμηρίωση, σαφήνεια μεθόδου, αναπαραγωγιμότητα όπου είναι εφικτό). Αντίθετα, “κίτρινη” βιβλιογραφία (yellow literature) όπως blogs και μη-τεκμηριωμένες διαδικτυακές αναρτήσεις δεν εντάσσεται στην τελική ανασκόπηση.

Στη συνέχεια παρουσιάζονται διαγράμματα που αποτυπώνουν την κατανομή των τελικών επιλεγμένων εργασιών ως προς: (α) το είδος δημοσίευσης, (β) τον εκδότη και (γ) το έτος δημοσίευσης.



Εικόνα 6: Κατανομή επιλεγμένων πηγών ανά είδος δημοσίευσης

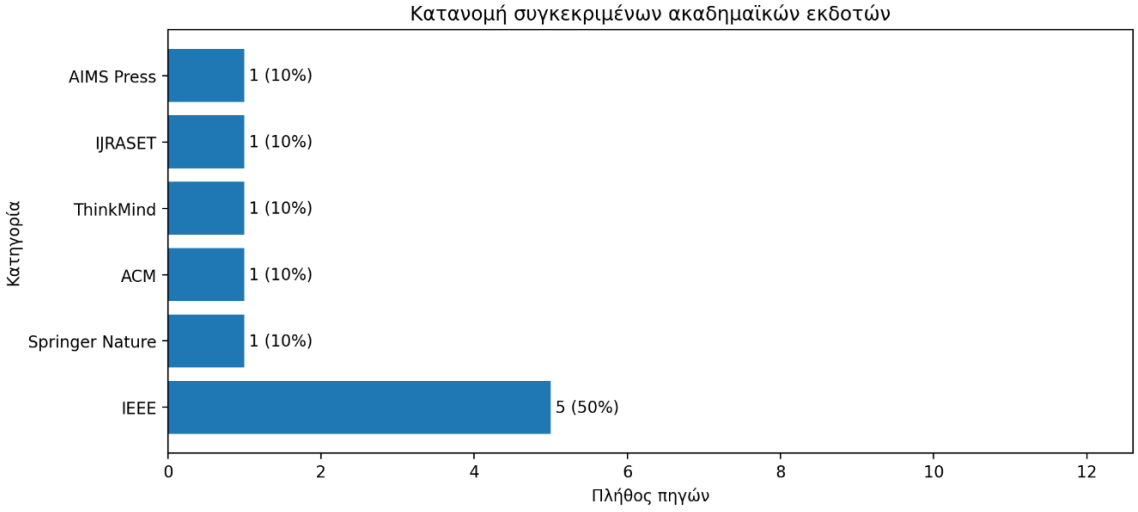
Η κατανομή των επιλεγμένων πηγών δείχνει ότι η τελική βιβλιογραφία προέρχεται κυρίως από άρθρα επιστημονικών περιοδικών και δημοσιεύσεις σε πρακτικά συνεδρίων, γεγονός που ενισχύει την αξιοπιστία και τη συγκρισιμότητα της ανάλυσης. Ειδικότερα, τα επιστημονικά άρθρα (σε περιοδικά και συνέδρια) αποτελούν το 46% του συνόλου των τελικών εργασιών. Παράλληλα, ενσωματώθηκαν επιλεκτικά τεχνικές αναφορές και working papers/pre-prints (π.χ. arXiv working papers, EBSE technical reports), καθώς και περιορισμένος αριθμός διαδικτυακών πηγών αποκλειστικά τύπου “grey literature”, δηλαδή επίσημα white papers και επίσημη τεκμηρίωση πλατφορμών (π.χ. Ethereum white paper, Hyperledger Fabric docs, Corda/Quorum/Ripple documentation), μόνο όταν παρείχαν σαφή μεθοδολογία, επαρκή τεχνική τεκμηρίωση ή κρίσιμη υποστήριξη σε ορισμούς και πρακτικά παραδείγματα.



Εικόνα 7: Κατανομή επιλεγμένων πηγών ανά είδος εκδότη/πλατφόρμα

Η κατανομή των πηγών ανά είδος εκδότη/πλατφόρμας δείχνει ότι το μεγαλύτερο μέρος του υλικού προέρχεται από ακαδημαϊκούς εκδότες και ψηφιακές βιβλιοθήκες (45%), γεγονός που υποδηλώνει ισχυρή παρουσία τυπικών επιστημονικών καναλιών δημοσίευσης στο τελικό σώμα της βιβλιογραφίας. Ακολουθούν οι ιδιωτικές εταιρείες με 23%, ενώ οι προδημοσιεύσεις σε αποθετήρια όπως το arXiv αντιστοιχούν στο 14%. Μικρότερη αλλά υπαρκτή είναι η συμμετοχή πηγών από ιδρύματα (foundations) και open-source consortia (9%) καθώς και από ερευνητικά ιδρύματα και πανεπιστήμια (9%). Συνολικά, η εικόνα δείχνει ότι η βιβλιογραφική βάση της εργασίας στηρίζεται κυρίως σε ακαδημαϊκούς εκδότες & ψηφιακές βιβλιοθήκες, αλλά συμπληρώνεται και από τεχνική τεκμηρίωση και υλικό προερχόμενο από φορείς με άμεση σχέση με την εφαρμογή των τεχνολογιών του πεδίου.

Πίνακας 4: Κατανομή από συγκεκριμένους ακαδημαϊκούς εκδότες



Στο Πίνακας 4: Κατανομή από συγκεκριμένους ακαδημαϊκούς εκδότες παρουσιάζεται η κατανομή των συγκεκριμένων ακαδημαϊκών εκδοτών που εντοπίστηκαν στο δείγμα. Η IEEE εμφανίζεται συχνότερα, με 5 πηγές (50%), ενώ οι Springer Nature, ACM, ThinkMind, IJRASET και AIMS Press καταγράφονται από 1 πηγή η καθεμία (10% έκαστος). Το εύρημα αυτό δείχνει ότι, παρότι υπάρχει κάποια διασπορά ως προς τους εκδότες, η IEEE καταλαμβάνει σαφώς πιο κεντρική θέση στο συγκεκριμένο σύνολο πηγών.

Εικόνα 8: Κατανομή επιλεγμένων πηγών ανά έτος δημοσίευσης

Πίνακας 5: Κατανομή επιλεγμένων πηγών ανά χρονικές περιόδους

Περίοδος	Πλήθος	Ποσοστό
2016–2018 (πρώτη ωρίμανση fog/edge & DLT)	9	40.9%
2019–2021 (έντονη ερευνητική δραστηριότητα)	9	40.9%
2022–2025 (πρόσφατη/τρέχουσα βιβλιογραφία)	4	18.2%

Η χρονική κατανομή των επιλεγμένων εργασιών δείχνει ότι η βιβλιογραφία κατανέμεται κυρίως στις περιόδους 2016–2018 και 2019–2021, οι οποίες συγκεντρώνουν από 9 εργασίες η καθεμία (40,9% αντίστοιχα). Το εύρημα αυτό υποδηλώνει ότι η συστηματική ερευνητική δραστηριότητα γύρω από τα περιβάλλοντα fog και edge computing, καθώς και τα ζητήματα ασφάλειας, ιδιωτικότητας και αξιοποίησης του blockchain, παρουσιάζει ιδιαίτερη ένταση σε

όλο το διάστημα 2016–2021. Σε επίπεδο επιμέρους ετών, το 2016 εμφανίζει τη μεγαλύτερη συγκέντρωση πηγών, ενώ η περίοδος 2019–2021 διατηρεί σταθερά υψηλή παρουσία δημοσιεύσεων, γεγονός που δείχνει τη συνεχιζόμενη ωρίμανση και ερευνητική εδραίωση του πεδίου. Αντίθετα, για την περίοδο 2022–2025 καταγράφονται 4 εργασίες (18,2%), στοιχείο που δείχνει μικρότερη αλλά υπαρκτή πρόσφατη βιβλιογραφική παρουσία στο τελικό σώμα πηγών. Σημειώνεται, όμως, πως επειδή η βιβλιογραφική αναζήτηση και φιλτάρισμα διενεργήθηκαν στην αρχή του 2025, ενδέχεται ορισμένα άρθρα που έγιναν δεκτά το 2024 να μην είχαν δημοσιευθεί ακόμη ενώ πολλά αδημοσίευτα άρθρα του 2025 να έχουν παραλειφθεί. Συνεπώς, αναμένουμε πως ο αριθμός των 4 εργασιών ενδέχεται να είναι μεγαλύτερος. Άρα, παρατηρούμε εν τέλει μια σταθερή ένταση έρευνας από το 2016 και έπειτα, η οποία υποδεικνύει το έντονο ερευνητικό ενδιαφέρον για τις τεχνολογίες που πραγματεύεται η εργασία μας.

4. Ζητήματα Ασφάλειας και Ιδιωτικότητας στο Fog και Edge Computing

4.1. Ζητήματα ασφάλειας

Το fog computing εισάγει μια νέα, αποκεντρωμένη υπολογιστική αρχιτεκτονική που φέρνει την επεξεργασία δεδομένων πιο κοντά στις πηγές δημιουργίας τους, βελτιώνοντας την απόκριση και περιορίζοντας την ανάγκη μετάδοσης μεγάλου όγκου δεδομένων προς το cloud. Ωστόσο, η γεωγραφική διασπορά, η ετερογένεια των συσκευών και η απουσία σταθερού ελέγχου δημιουργούν ένα τοπίο με νέες και επιτακτικές απαιτήσεις ασφάλειας. Τα ζητήματα αυτά διακρίνονται σε δύο κύριες κατηγορίες: τις τρωτότητες των υποδομών και τις ενεργές επιθέσεις που επιχειρούν να τις εκμεταλλευτούν.

4.1.1 Τρωτότητες (Vulnerabilities)

Η πρώτη και θεμελιώδης πρόκληση στα περιβάλλοντα fog και edge computing αφορά τις ενδογενείς τρωτότητες των ίδιων των υποδομών, οι οποίες μπορούν να καταστήσουν τα συστήματα ευάλωτα σε επιθέσεις ακόμη και χωρίς άμεση ανθρώπινη παρέμβαση. Οι τρωτότητες αυτές δεν εμφανίζονται αποσπασματικά, αλλά μπορούν να οργανωθούν σε ευρύτερες κατηγορίες, οι οποίες αφορούν την ετερογένεια των συσκευών και του λογισμικού, τις τεχνολογίες δοχειοποίησης και ορχήστρωσης, τα πρωτόκολλα επικοινωνίας, τις διαχειριστικές διεπαφές, τις διαδικασίες ενημέρωσης, τη διαχείριση εμπιστοσύνης, καθώς και ζητήματα φυσικής και οργανωτικής ασφάλειας. Για τον λόγο αυτό, προχωρούμε σε μια ιεραρχική κατηγοριοποίηση των βασικών τρωτοτήτων στα περιβάλλοντα fog και edge computing, η οποία αναλύεται στις επόμενες υποενότητες και απεικονίζεται συνοπτικά στην Εικόνα 9: Τρωτότητες .

4.1.1.1 Ετερογένεια Συσκευών / Κόμβων

Μία τέτοια αδυναμία είναι η ετερογένεια των συσκευών: οι κόμβοι ομίχλης (fog) — όπως και πολλοί κόμβοι/συσκευές ακμής — ενδέχεται να χρησιμοποιούν διαφορετικά λειτουργικά συστήματα, βιβλιοθήκες λογισμικού, και εκδόσεις υλισμικού (firmware). Η ετερογένεια αυτή αυξάνει την επιφάνεια επίθεσης (attack surface), καθώς κάθε διαφορετικό στοιχείο λογισμικού ή υλικού μπορεί να εισάγει ξεχωριστές ευπάθειες.

Σε περιβάλλοντα χωρίς ομοιομορφία, η διαδικασία ενημέρωσης και επιδιόρθωσης (patch management) καθίσταται πιο πολύπλοκη και λιγότερο συντονισμένη, με αποτέλεσμα ορισμένοι κόμβοι να παραμένουν σε παλαιότερες ή μη ασφαλείς εκδόσεις. Αυτό ισχύει τόσο σε fog κόμβους (λόγω διαφορετικών παρόχων/τοποθεσιών) όσο και στο edge (λόγω πλήθους και διασποράς συσκευών). Έτσι, αυξάνεται η πιθανότητα ύπαρξης μη επιδιορθωμένων ευπαθειών τύπου CVE (Common Vulnerabilities and Exposures). Βέβαια υπάρχει και το ενδεχόμενο zero-day ευπαθειών, οι οποίες δεν έχουν ακόμη εντοπιστεί ή διορθωθεί [2]. Αντίθετα, σε περισσότερο ομοιογενείς υποδομές είναι εφικτή η υιοθέτηση ενιαίων, επικαιροποιημένων και

αυστηρά ελεγχόμενων εκδόσεων λογισμικού, γεγονός που διευκολύνει την κεντρική διαχείριση ασφάλειας.

4.1.1.2 Τρωτότητες Εικονικοποίησης, Δοχειοποίησης και Ορχήστρωσης

Επιπλέον, πολλές πλατφόρμες fog βασίζονται στη δοχειοποίηση (containerization) και σε τεχνολογίες όπως Docker ή Kubernetes για την απομόνωση υπηρεσιών. Παρόμοιες τεχνολογίες απαντώνται και σε ενδιάμεσους/ισχυρότερους edge κόμβους (π.χ. gateways), όπου εκτελούνται πολλαπλά workloads. Αν και η δοχειοποίηση προσφέρει λειτουργικά πλεονεκτήματα, εισάγει ένα επιπλέον επίπεδο πολυπλοκότητας και, συνεπώς, νέες κατηγορίες τρωτοτήτων.

Οι τρωτότητες αυτές μπορούν να διακριθούν σε τρεις βασικές κατηγορίες:

(α) Λανθασμένες διαμορφώσεις (misconfigurations):

Σε περιπτώσεις εσφαλμένης ρύθμισης, containers μπορεί να εκτελούνται με αυξημένα δικαιώματα (π.χ. run as root), να διαθέτουν πρόσβαση σε host resources (volume mounts, host networking) ή να εκτίθενται μέσω μη προστατευμένων APIs. Παρόμοια προβλήματα περιλαμβάνουν την απουσία περιορισμών (resource limits), τη μη χρήση μηχανισμών απομόνωσης (namespaces, cgroups) την ανεπαρκή πολιτική πρόσβασης καθώς και την κακή διαχείριση μυστηκών (secrets), όπως η αποθήκευση σε plain text.

(β) Τρωτότητες επιπέδου απομόνωσης και runtime:

Η απομόνωση των containers δεν είναι ισοδύναμη με την απομόνωση εικονικών μηχανών (VMs), καθώς μοιράζονται τον ίδιο kernel με το host. Τρωτότητες στον kernel ή στο container runtime (π.χ. container escape vulnerabilities) μπορούν να επιτρέψουν σε έναν επιτιθέμενο να αποκτήσει πρόσβαση στο host σύστημα (ακόμη και root – αυτό εξαρτάται από το πως έχει διαμορφωθεί το εκτελούμενο δοχείο).

(γ) Τρωτότητες orchestrator και εφοδιαστικής αλυσίδας (supply chain risks):

Σε περιβάλλοντα Kubernetes, τρωτότητες μπορεί να εντοπίζονται:

- Στον ίδιο τον orchestrator (π.χ. αδύναμο RBAC configuration)
- Σε εκτεθειμένα control-plane APIs
- Στη χρήση μη αξιόπιστων ή ευάλωτων base images
- Στη μη υπογεγραμμένη ή μη ελεγμένη προέλευση container images

Η χρήση δημόσιων αποθετηρίων (repositories) χωρίς επαλήθευση της ακεραιότητας των images αυξάνει τον κίνδυνο εισαγωγής κακόβουλου

λογισμικού, ενώ η απουσία πολιτικών ασφαλούς διαχείρισης μυστικών (secrets management) μπορεί να οδηγήσει σε διαρροή διαπιστευτηρίων.

Συνεπώς, η δοχειοποίηση στο fog computing δεν δημιουργεί μόνο κινδύνους λόγω λανθασμένων ρυθμίσεων, αλλά εισάγει ένα ευρύτερο οικοσύστημα πιθανών τρωτοτήτων που εκτείνονται από το επίπεδο runtime μέχρι τον μηχανισμό ορχήστρωσης και την αλυσίδα εφοδιασμού λογισμικού.

4.1.1.3 Τρωτότητες Πρωτοκόλλων και Ασφαλούς Επικοινωνίας

Ένα ακόμη κρίσιμο πεδίο τρωτότητας αφορά τα πρωτόκολλα ασφαλούς επικοινωνίας, όπως το TLS ή το DTLS, τα οποία συχνά θεωρούνται «δεδομένα» ότι παρέχουν προστασία. Ωστόσο, η ασφάλεια που παρέχουν εξαρτάται σε μεγάλο βαθμό από τον τρόπο υλοποίησης, διαμόρφωσης και ενσωμάτωσής τους στην αρχιτεκτονική του συστήματος (τόσο σε fog όσο και σε edge περιβάλλοντα).

Οι αδυναμίες/τρωτότητες μπορούν να διακριθούν σε τρεις κατηγορίες:

(α) Τρωτότητες υλοποίησης (implementation vulnerabilities):

Σφάλματα σε βιβλιοθήκες κρυπτογράφησης ή στον τρόπο ενσωμάτωσης του TLS/DTLS (π.χ. buffer overflows, memory leaks, logic errors) μπορεί να επιτρέψουν επιθέσεις, ακόμη και όταν το πρωτόκολλο θεωρητικά είναι ασφαλές.

(β) Ζητήματα διαμόρφωσης και επιχειρησιακής πρακτικής (misconfiguration / operational weaknesses):

Η χρήση παρωχημένων εκδόσεων (π.χ. TLS 1.0), deprecated αλγορίθμων, αδύναμων cipher suites ή η κακή χρήση πιστοποιητικών (π.χ. μη επαλήθευση πιστοποιητικών, αποδοχή self-signed certificates, μη ενεργοποίηση certificate validation) υπονομεύει την ασφάλεια της επικοινωνίας.

(γ) Σχεδιαστικές επιλογές (design decisions):

Σε ορισμένες περιπτώσεις, η μη υιοθέτηση κοινής αυθεντικοποίησης (mutual authentication) ή καρφιτσώματος πιστοποιητικών (certificate pinning) αποτελεί αρχιτεκτονική επιλογή που μειώνει το επίπεδο προστασίας έναντι επιθέσεων τύπου Man-in-the-Middle.

Συνεπώς, το πρόβλημα δεν εντοπίζεται στο ίδιο το πρωτόκολλο, αλλά στον τρόπο με τον οποίο αυτό υλοποιείται, ρυθμίζεται και ενσωματώνεται στο εκάστοτε fog (ή edge/IoT) περιβάλλον. Σχετικές αναφορές επισημαίνουν ότι οι επιθέσεις τύπου υποβάθμισης (downgrade), πλαστοπροσωπίας (spoofing) ή έκχυσης πιστοποιητικών (certificate injection) έχουν εμφανιστεί ακόμη και σε περιβάλλοντα fog/IoT με υποτιθέμενη χρήση TLS, γεγονός που αποδεικνύει ότι η ύπαρξη του πρωτοκόλλου δεν συνεπάγεται κατ’ ανάγκη και ορθή ή ασφαλή χρήση του [2].

4.1.1.4 Τρωτότητες Διαχειριστικών Διεπαφών και Μηχανισμών Ελέγχου

Σημαντική πηγή τρωτοτήτων αποτελούν επίσης οι διαχειριστικές διεπαφές (management interfaces) των κόμβων, ειδικά όταν είναι διαθέσιμες απομακρυσμένα μέσω web-based κονσολών ή REST APIs. Το ζήτημα αυτό αφορά τόσο fog κόμβους όσο και edge gateways/συσκευές που εκθέτουν αντίστοιχες διεπαφές διαχείρισης.

Οι σχετικές αδυναμίες μπορούν να διακριθούν σε τρεις βασικές κατηγορίες.

(α) Ζητήματα διαμόρφωσης και επιχειρησιακής πρακτικής (misconfiguration / operational weaknesses):

Η ύπαρξη ανοιχτών θυρών (open ports), η χρήση προεπιλεγμένων διαπιστευτηρίων (default credentials) ή η απουσία μηχανισμών rate-limiting εκθέτουν το σύστημα σε επιθέσεις brute-force ή αυτόματης σάρωσης (automated scanning). Επιπλέον, η έκθεση των διεπαφών διαχείρισης στο δημόσιο διαδίκτυο (χωρίς κατάλληλη δικτυακή απομόνωση, VPN ή περιορισμό πρόσβασης) μετατρέπει τα control panels και τα management APIs σε εύκολα ανιχνεύσιμους στόχους για μαζική σάρωση και στοχευμένες επιθέσεις. Τέλος, η έλλειψη καταγραφής συμβάντων (logging) και μηχανισμών παρακολούθησης δυσχεραίνει την έγκαιρη ανίχνευση ύποπτης δραστηριότητας και την απόδοση ευθύνης (accountability), επιτρέποντας σε επιτιθέμενους να παραμένουν στο σύστημα χωρίς να αφήνουν εμφανή ίχνη. Σε fog περιβάλλοντα με γεωγραφική διασπορά (και αντίστοιχα σε διασκορπισμένες edge εγκαταστάσεις), η μη σωστή σκλήρυνση (hardening) των διεπαφών αυξάνει σημαντικά την επιφάνεια επίθεσης.

(β) Αδυναμίες αυθεντικοποίησης και ελέγχου πρόσβασης (authentication & authorization weaknesses):

Ο ανεπαρκής έλεγχος ταυτοποίησης (weak authentication) ή η ελλιπής υλοποίηση role-based access control (RBAC) (έλεγχος πρόσβασης βάσει ρόλων) μπορεί να επιτρέψει σε μη εξουσιοδοτημένους χρήστες να αποκτήσουν διαχειριστικά δικαιώματα. Η απουσία multi-factor authentication (πολύ-παραγοντικής αυθεντικοποίησης) καθιστά εφικτή την κατάχρηση κλεμμένων ή διαρρεύσαντων διαπιστευτηρίων.

(γ) Τρωτότητες υλοποίησης (implementation vulnerabilities):

Σφάλματα στον κώδικα των διαχειριστικών εφαρμογών (πχ. έλειψη επικύρωσης εισόδου) μπορούν να οδηγήσουν σε injection ευπάθειες, όπως command injection ή SQL injection. Σε τέτοιες περιπτώσεις, ένας επιτιθέμενος μπορεί να εισάγει κακόβουλες εντολές μέσω πεδίων εισόδου, αποκτώντας έλεγχο του συστήματος ή εκτελώντας αυθαίρετο κώδικα στο επίπεδο του λειτουργικού συστήματος.

4.1.1.5 Τρωτότητες Ενημερώσεων, Συντήρησης και Κύκλου Ζωής Λογισμικού

Στα fog περιβάλλοντα, όπου οι κόμβοι συχνά λειτουργούν σε απομακρυσμένες ή μη πλήρως ελεγχόμενες τοποθεσίες, οι διαχειριστικές διεπαφές αποτελούν υψηλής αξίας στόχο (high-value target), καθώς παρέχουν άμεση πρόσβαση στον έλεγχο της υποδομής. Αντίστοιχα, στο edge η ύπαρξη εκτεθειμένων διεπαφών σε πολλαπλές συσκευές αυξάνει ακόμη περισσότερο τη δυνατότητα μαζικής εκμετάλλευσης. Συνεπώς, η ασφάλειά τους δεν εξαρτάται μόνο από την ορθή υλοποίηση, αλλά και από την αυστηρή διαμόρφωση και συνεχή παρακολούθησή τους [5].

Διακριτό πεδίο τρωτότητας αποτελούν επίσης οι διαδικασίες ενημέρωσης λογισμικού και firmware, οι οποίες σχετίζονται με τον κύκλο ζωής και τη συντήρηση των fog και edge κόμβων. Εκτός από την πρόκληση της έγκαιρης και καθολικής εφαρμογής patches σε όλους τους κόμβους, έχει αναγνωριστεί ότι οι μη ασφαλείς μηχανισμοί ενημέρωσης (π.χ. μη υπογεγραμμένα firmware updates ή απουσία integrity check) μπορούν να αποτελέσουν όχημα για την έκχυση κακόβουλου λογισμικού. Επιπλέον, η συχνή ένταξη/αποχώρηση κόμβων σε δυναμικά edge περιβάλλοντα δυσχεραίνει την αξιόπιστη πιστοποίηση και την επιβολή ενιαίων πολιτικών ενημέρωσης, αυξάνοντας τον κίνδυνο συμβιβασμού μέσω αδύναμου onboarding ή μη ασφαλών update διαδικασιών.

4.1.1.6 Τρωτότητες Διαχείρισης Εμπιστοσύνης και Συνεργασίας Κόμβων

Πέραν των επιμέρους τεχνικών τρωτοτήτων σε επίπεδο λογισμικού, πρωτοκόλλων και διαχειριστικών διεπαφών, ιδιαίτερα κρίσιμη είναι και η απουσία μηχανισμών διαχείρισης εμπιστοσύνης (trust management) μεταξύ των κόμβων της fog αρχιτεκτονικής. Σε αποκεντρωμένα και δυναμικά περιβάλλοντα (συμπεριλαμβανομένων και αντίστοιχων edge οικοσυστημάτων), οι κόμβοι αλληλεπιδρούν, ανταλλάσσουν δεδομένα και αναλαμβάνουν λειτουργίες χωρίς πάντοτε να υφίσταται ένας συνεχής και ποσοτικοποιημένος μηχανισμός αξιολόγησης της αξιοπιστίας τους.

Η έλλειψη δυναμικών μηχανισμών αξιολόγησης εμπιστοσύνης (π.χ. reputation systems, trust scoring, συνεχής επαλήθευση ταυτότητας ή zero-trust μοντέλα) μπορεί να επιτρέψει σε έναν παραβιασμένο κόμβο να συνεχίσει να θεωρείται «έμπιστος» από τους υπόλοιπους. Σε μια τέτοια περίπτωση, ο κόμβος αυτός δύναται να διαδώσει παραποιημένα δεδομένα, να αλλοιώσει αλγορίθμους κατανομής φορτίου, να επηρεάσει διαδικασίες συντονισμού ή να λειτουργήσει ως ενδιάμεσο σημείο διάδοσης κακόβουλης δραστηριότητας. Το πρόβλημα αποκτά συστημικό χαρακτήρα, καθώς η παραβίαση δεν περιορίζεται τοπικά, αλλά δύναται να επηρεάσει πολλαπλά επίπεδα της υποδομής αν δεν υπάρχει κατάλληλη τμηματοποίησή της.

Επιπλέον, σε περιβάλλοντα fog όπου εφαρμόζονται μηχανισμοί συνεργατικής επεξεργασίας ή δυναμικής ανακατεύθυνσης εργασιών (task offloading), η

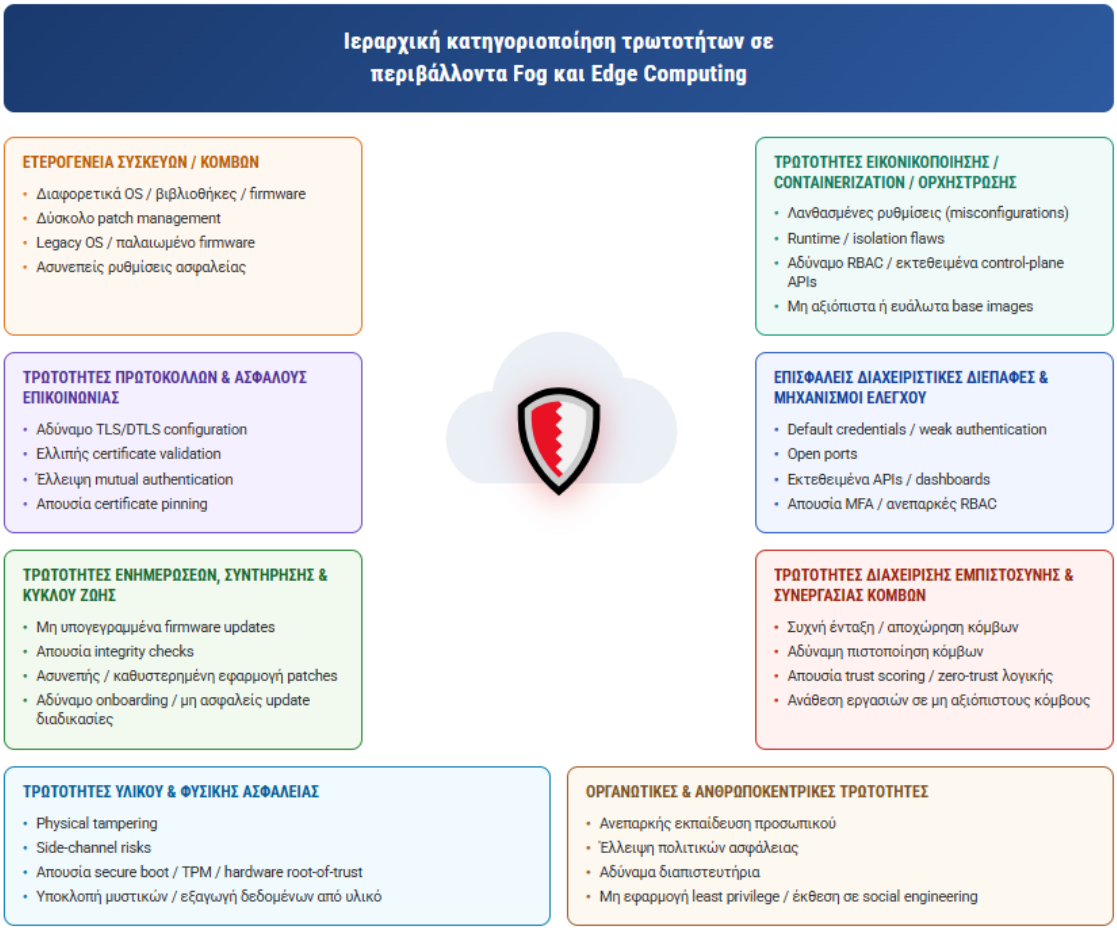
απουσία αξιόπιστης διαχείρισης εμπιστοσύνης ενδέχεται να οδηγήσει σε ανάθεση κρίσιμων λειτουργιών σε μη αξιόπιστους κόμβους. Αυτό αυξάνει την πιθανότητα αλλοίωσης δεδομένων, διαρροής πληροφορίας ή εσκεμμένης υποβάθμισης της απόδοσης (performance degradation). Συνεπώς, η διαχείριση εμπιστοσύνης δεν αποτελεί απλώς μηχανισμό βελτίωσης της ασφάλειας, αλλά δομικό στοιχείο για τη διατήρηση της συνολικής ανθεκτικότητας (resilience) της fog αρχιτεκτονικής.

4.1.1.7 Τρωτότητες Υλικού και Φυσικής Ασφάλειας

Πέραν των ευπαθειών λογισμικού, οι υποδομές fog είναι εκτεθειμένες και σε τρωτότητες επιπέδου υλικού και οργανωτικής διαχείρισης. Σε επίπεδο υλικού, οι κόμβοι ομίχλης συχνά εγκαθίστανται σε γεωγραφικά διασκορπισμένα ή μη πλήρως ελεγχόμενα περιβάλλοντα (π.χ. βιομηχανικές εγκαταστάσεις, αστικά σημεία, υποδομές έξυπνων πόλεων), γεγονός που τους καθιστά ευάλωτους σε φυσική παραβίαση (physical tampering), επιθέσεις πλευρικού καναλιού (side-channel attacks), καθώς και σε κακόβουλη τροποποίηση firmware ή hardware components. Αντίστοιχα, στο edge ο κίνδυνος φυσικής παραβίασης είναι εντονότερος, καθώς πολλές συσκευές λειτουργούν σε δημόσια ή μη επιτηρούμενα σημεία. Η απουσία μηχανισμών secure boot, trusted platform modules (TPM) ή hardware root-of-trust, καθώς και η έλλειψη hardware-assisted trust σε αρκετές πλατφόρμες, μπορεί να επιτρέψει την εκτέλεση μη εξουσιοδοτημένου κώδικα σε επίπεδο συστήματος ή την υποκλοπή μυστικών [17].

4.1.1.8 Οργανωτικές και Ανθρωποκεντρικές Τρωτότητες

Επιπλέον, ιδιαίτερα κρίσιμες είναι οι οργανωτικές και ανθρώπινες τρωτότητες. Η ανεπαρκής εκπαίδευση προσωπικού, η έλλειψη πολιτικών ασφάλειας, τα αδύναμα διαπιστευτήρια και η μη εφαρμογή αρχών ελάχιστων προνομίων (least privilege) δημιουργούν ευνοϊκό περιβάλλον για επιθέσεις κοινωνικής μηχανικής (social engineering). Τεχνικές όπως phishing, spear phishing ή credential harvesting μπορούν να οδηγήσουν σε παραβίαση διαχειριστικών λογαριασμών, παρακάμπτοντας πλήρως τους τεχνικούς μηχανισμούς προστασίας του συστήματος. Στα fog και edge περιβάλλοντα, όπου η διαχείριση πραγματοποιείται συχνά απομακρυσμένα και από πολλαπλούς φορείς, η ανθρώπινη διάσταση της ασφάλειας καθίσταται εξίσου κρίσιμη με την τεχνική θωράκιση.



Εικόνα 9: Τρωτότητες σε περιβάλλοντα ομίχλης και ακμών

4.1.2 Επιθέσεις (Attacks)

Οι παραπάνω τρωτότητες αξιοποιούνται ενεργά από κακόβουλους παράγοντες μέσω στοχευμένων επιθέσεων, οι οποίες εκδηλώνονται σε διαφορετικά επίπεδα των fog και edge υποδομών. Οι επιθέσεις αυτές δεν περιορίζονται μόνο στην παρεμβολή της επικοινωνίας, αλλά περιλαμβάνουν επιθέσεις διαθεσιμότητας, γενικές δικτυακές και ασύρματες επιθέσεις, επιθέσεις σε επίπεδο εφαρμογής και διαχειριστικών διεπαφών, επιθέσεις που βασίζονται σε διαπιστευτήρια, επιθέσεις εφοδιαστικής αλυσίδας, επιθέσεις εμπιστοσύνης, επιθέσεις φυσικής πρόσβασης, side-channel επιθέσεις, καθώς και επιθέσεις στην ακεραιότητα των υπολογισμών. Για λόγους συστηματικής ανάλυσης, οι βασικές αυτές κατηγορίες, τα υπο-είδη τους, οι στόχοι τους και οι κύριες επιπτώσεις τους ως προς την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα παρουσιάζονται συνοπτικά στον Πίνακας 6: Κατηγοριοποίηση Επιθέσεων σε Fog και Edge Περιβάλλοντα καθώς και στην Εικόνα 10: Επιθέσεις σε fog/edge περιβάλλοντα και αναλύονται διεξοδικά στις υποενότητες που ακολουθούν.

4.1.2.1 Επιθέσεις Παρεμβολής Επικοινωνίας (Man-in-the-Middle – MITM)

Η επίθεση MITM λαμβάνει χώρα όταν ένας επιτιθέμενος παρεμβάλλεται μεταξύ δύο επικοινωνούντων οντοτήτων (π.χ. κόμβος fog και edge συσκευή), χωρίς αυτές να το αντιλαμβάνονται. Ο επιτιθέμενος αποκτά τη δυνατότητα να παρακολουθεί, να τροποποιεί ή να ανακατευθύνει την επικοινωνία [2].

Υπο-είδη MITM

Η MITM δεν αποτελεί ενιαία τεχνική αλλά περιλαμβάνει επιμέρους μορφές:

(α) Eavesdropping (Παθητική Υποκλοπή)

Ο επιτιθέμενος παρακολουθεί την κυκλοφορία χωρίς να την τροποποιεί.

Επιπτώσεις:

- Παραβίαση εμπιστευτικότητας
- Διαρροή ευαίσθητων δεδομένων
- Αποκάλυψη credentials ή tokens

(β) Active MITM / Data Tampering

Ο επιτιθέμενος τροποποιεί ενεργά τα δεδομένα κατά τη μεταφορά.

Επιπτώσεις:

- Παραποίηση εντολών ελέγχου
- Εσφαλμένη λήψη αποφάσεων σε real-time εφαρμογές
- Εισαγωγή κακόβουλων payloads

(γ) Downgrade Attacks

Ο επιτιθέμενος εξαναγκάζει τα δύο άκρα να χρησιμοποιήσουν παλαιότερη, λιγότερο ασφαλή έκδοση πρωτοκόλλου ή αλγορίθμου.

Επιπτώσεις:

- Αποδυνάμωση κρυπτογράφησης
- Ευκολότερο «σπάσιμο» της κρυπτογράφησης για την αποκάλυψη των δεδομένων (στον επιτιθέμενο)

(δ) Spoofing & Certificate Injection

Ο επιτιθέμενος προσποιείται νόμιμο κόμβο μέσω ψευδούς πιστοποιητικού ή παραποίησης ταυτότητας, ώστε να γίνει αποδεκτός ως έμπιστος συμμετέχων από άλλους κόμβους ή συσκευές. Έτσι αποκτά τη δυνατότητα να παρεμβάλλεται στην επικοινωνία, να υποκλέπτει δεδομένα ή να ανακατευθύνει τη ροή τους χωρίς να γίνεται άμεσα αντιληπτός.

Επιπτώσεις:

- Μη εξουσιοδοτημένη πρόσβαση
- Κατάληψη session (session hijacking)
- Παραπλάνηση συσκευών edge

4.1.2.2 Physical Tampering / Device Capture (Φυσική παραβίαση & κατάληψη συσκευής)

Ιδιαίτερα στο edge—όπου οι συσκευές βρίσκονται συχνά σε δημόσια ή μη επιτηρούμενα σημεία—η φυσική πρόσβαση επιτρέπει επιθέσεις τύπου tampering που οδηγούν σε εξαγωγή δεδομένων/κλειδιών, αποσφαλμάτωση μέσω φυσικών διεπαφών (π.χ. UART/JTAG), dump μνήμης ή ακόμη και πλήρη αντικατάσταση λογισμικού/firmware. Παρόμοια περιστατικά είναι εφικτά και σε fog κόμβους όταν αυτοί εγκαθίστανται σε απομακρυσμένες ή ημι-ελεγχόμενες τοποθεσίες (π.χ. υποδομές έξυπνων πόλεων, βιομηχανικά σημεία), λειτουργώντας ως “ενδιάμεσες” υποδομές. Οι επιθέσεις αυτές μπορούν να οδηγήσουν σε εγκατάσταση κακόβουλων modules, αλλοίωση αισθητηριακών μετρήσεων σε πραγματικό χρόνο και υποκλοπή κρυπτογραφικών μυστικών, με άμεσο αντίκτυπο στην ακεραιότητα και τη διαθεσιμότητα υπηρεσιών [17].

4.1.2.3 Επιθέσεις Άρνησης Εξυπηρέτησης και Εξάντλησης Πόρων (Denial-of-Service, Distributed DoS και Resource Exhaustion Attacks)

Ένα ιδιαίτερα σημαντικό είδος απειλής είναι οι επιθέσεις άρνησης εξυπηρέτησης (DoS) και οι κατανεμημένες παραλλαγές τους (DDoS). Στα fog περιβάλλοντα, οι επιθέσεις αυτές δεν εκδηλώνονται πάντοτε ως μεμονωμένα

γεγονότα, αλλά συχνά εντάσσονται σε σύνθετες, πολυσταδιακές επιθετικές αλυσίδες (multi-stage attacks). Συγκεκριμένα, οι επιτιθέμενοι στοχεύουν αρχικά σε τελικές IoT συσκευές, αξιοποιώντας γνωστές ή ευπάθειες μηδενικής ημέρας (zero-day vulnerabilities), αδύναμα διαπιστευτήρια, ανοιχτές θύρες ή ελλιπείς μηχανισμούς αυθεντικοποίησης, με σκοπό την ανατροπή του ελέγχου τους (device compromise).

Η κατάληψη IoT συσκευών μπορεί να επιτευχθεί μέσω επιθέσεων brute-force σε default credentials, exploitation ευπαθειών firmware, buffer overflow επιθέσεων, command injection σε web-based διεπαφές ή ακόμη και μέσω κακόβουλων ενημερώσεων λογισμικού. Αφού αποκτήσουν έλεγχο μεγάλου αριθμού συσκευών, οι επιτιθέμενοι τις εντάσσουν σε botnets, τα οποία χρησιμοποιούνται ως κατανεμημένες πλατφόρμες εκτόξευσης DDoS επιθέσεων προς κόμβους fog ή cloud.

Η περίπτωση του Mirai botnet αποτελεί χαρακτηριστικό παράδειγμα αυτής της στρατηγικής, καθώς αξιοποίησε αδύναμες IoT συσκευές (π.χ. κάμερες και routers) για τη δημιουργία ενός εκτεταμένου δικτύου bots, προκαλώντας μαζικές διακοπές υπηρεσιών σε κρίσιμες υποδομές [5]. Το κρίσιμο στοιχείο στις επιθέσεις αυτού του τύπου είναι η κλίμακα: οι IoT συσκευές είναι πολυπληθείς, γεωγραφικά διασκορπισμένες και συχνά ανεπαρκώς προστατευμένες. Επομένως, η ταυτόχρονη κατάληψη μεγάλου αριθμού τέτοιων συσκευών μπορεί να δημιουργήσει ιδιαίτερα υψηλό όγκο κακόβουλης κίνησης, ικανό να παραλύσει fog κόμβους με περιορισμένους υπολογιστικούς και δικτυακούς πόρους αλλά ακόμη και να οδηγήσει σε μη διαθεσιμότητα πολλές υπηρεσίες νέφους.

Οι επιπτώσεις μιας επιτυχημένης DDoS επίθεσης σε fog περιβάλλον περιλαμβάνουν υποβάθμιση ή πλήρη απώλεια διαθεσιμότητας (availability), διακοπή υπηρεσιών σε πραγματικό χρόνο, καθυστέρηση κρίσιμων αποφάσεων σε βιομηχανικά ή υγειονομικά συστήματα, καθώς και αλυσιδωτή επιβάρυνση ανώτερων επιπέδων (cloud) λόγω επαναδρομολόγησης αιτημάτων. Συνεπώς, οι DoS/DDoS επιθέσεις σε fog αρχιτεκτονικές δεν συνιστούν απλώς ζήτημα υπερφόρτωσης δικτύου, αλλά εντάσσονται σε ευρύτερες στρατηγικές εκμετάλλευσης της κλίμακας και της ετερογένειας του οικοσυστήματος IoT, με δυνητικά σοβαρές επιπτώσεις στη λειτουργική συνέχεια των παρεχόμενων υπηρεσιών [5].

Παράλληλα, σε περιβάλλοντα edge (και σε ενεργειακά/υπολογιστικά περιορισμένους κόμβους fog), οι επιθέσεις άρνησης εξυπηρέτησης δεν περιορίζονται στο “flooding” (πλημμύρισμα) δικτύου: εμφανίζονται και ως επιθέσεις εξάντλησης πόρων (resource exhaustion) ή/και battery-drain, όπου ο επιτιθέμενος προκαλεί συνεχείς υπολογισμούς, επαναλαμβανόμενες συνδέσεις ή τεχνητά αυξημένο φόρτο, οδηγώντας σε ταχεία κατανάλωση ενέργειας, υπερθέρμανση ή υποβάθμιση QoS [17].

4.1.2.4 Δικτυακές Επιθέσεις και Επιθέσεις σε Ασύρματα Μέσα Μετάδοσης (Network and Wireless Communication Attacks)

Εκτός από τις επιθέσεις άρνησης εξυπηρέτησης, σημαντική κατηγορία απειλών αφορά τις δικτυακές επιθέσεις που στοχεύουν τη μετάδοση δεδομένων. Οι επιθέσεις αυτές μπορούν να διακριθούν σε δύο βασικές κατηγορίες: (α) γενικές δικτυακές επιθέσεις, που αφορούν τόσο ενσύρματα όσο και ασύρματα περιβάλλοντα, και (β) επιθέσεις που στοχεύουν ειδικά ασύρματα δίκτυα, τα οποία είναι ιδιαίτερα διαδεδομένα σε IoT και fog αρχιτεκτονικές.

(α) Γενικές δικτυακές επιθέσεις

Replay Attacks (Επιθέσεις επανάληψης):

Σε μια επίθεση replay, ο επιτιθέμενος καταγράφει έγκυρα πακέτα δεδομένων που μεταδίδονται μεταξύ δύο κόμβων και τα επαναμεταδίδει σε μεταγενέστερο χρόνο. Εάν δεν εφαρμόζονται μηχανισμοί όπως nonce values, timestamps ή sequence numbers, το σύστημα ενδέχεται να αποδεχθεί το παλαιό πακέτο ως έγκυρο.

Επιπτώσεις:

- Εκτέλεση παλαιών εντολών ελέγχου
- Παραποίηση κατάστασης συστήματος
- Εσφαλμένη λήψη αποφάσεων σε real-time εφαρμογές

Packet Injection:

Σε αυτή την περίπτωση, ο επιτιθέμενος εισάγει κακόβουλα ή παραποιημένα πακέτα στο δίκτυο, προσποιούμενος νόμιμο κόμβο. Η επιτυχία της επίθεσης εξαρτάται από αδυναμίες αυθεντικοποίησης ή ελέγχου ακεραιότητας. Σε ορισμένες περιπτώσεις, τα πακέτα αυτά μπορεί να είναι ειδικά διαμορφωμένα ώστε να εκμεταλλεύονται αδυναμίες πρωτοκόλλων ή του λειτουργικού συστήματος, οδηγώντας ακόμη και σε άρνηση εξυπηρέτησης (DoS), όπως σε επιθέσεις τύπου packet/ping of death.

Επιπτώσεις:

- Παραποίηση δεδομένων αισθητήρων
- Εισαγωγή ψευδών σημάτων ελέγχου
- Αποσταθεροποίηση αλγορίθμων ανάλυσης ή AI/ML
- Πρόκληση DoS ή δυσλειτουργίας συστήματος

Reflection Attacks (Επιθέσεις ανάκλασης):

Οι επιθέσεις ανάκλασης αποτελούν ειδική μορφή DoS/DDoS, κατά την οποία ο επιτιθέμενος δεν στέλνει απευθείας όλη την κακόβουλη κίνηση στο θύμα, αλλά αξιοποιεί ενδιάμεσους εξυπηρετητές ή υπηρεσίες τρίτων ως «ανακλαστήρες» (reflectors). Ειδικότερα, αποστέλλει αιτήματα με παραποιημένη διεύθυνση πηγής, έτσι ώστε οι απαντήσεις των τρίτων συστημάτων να καταλήγουν στο θύμα, προκαλώντας υπερφόρτωση δικτυακών ή υπολογιστικών πόρων. Όταν οι απαντήσεις είναι πολύ μεγαλύτερες από τα αρχικά αιτήματα, προκύπτει και φαινόμενο ενίσχυσης (amplification), το οποίο αυξάνει σημαντικά την ένταση της επίθεσης. Σε fog και edge περιβάλλοντα, τέτοιες επιθέσεις μπορούν να πλήξουν κυρίως gateways, ενδιάμεσους κόμβους ή υποδομές ελέγχου με περιορισμένους πόρους, οδηγώντας σε σοβαρή υποβάθμιση της διαθεσιμότητας.

Επιπτώσεις:

- Υπερφόρτωση δικτυακών και υπολογιστικών πόρων
- Υποβάθμιση ή διακοπή υπηρεσιών
- Αδυναμία εξυπηρέτησης νόμιμων αιτημάτων
- Ενίσχυση της επίθεσης μέσω amplification mechanisms

(β) Επιθέσεις σε ασύρματα δίκτυα

Σε fog/IoT περιβάλλοντα, μεγάλο μέρος της επικοινωνίας πραγματοποιείται μέσω Wi-Fi, LTE/5G, ZigBee, LoRa ή άλλων ασύρματων τεχνολογιών. Η φύση των ασύρματων μέσων (ανοιχτή διάδοση σήματος) εισάγει πρόσθετες τρωτότητες.

Jamming Attacks:

Ο επιτιθέμενος εκπέμπει ισχυρό ή συνεχές σήμα στην ίδια συχνότητα με το δίκτυο-στόχο, παρεμποδίζοντας την ομαλή μετάδοση. Αυτό το είδος επίθεσης θα μπορούσε να θεωρηθεί και τύπου DoS, ειδικότερα όσον αφορά τις 2 από τις 3 παρακάτω επιπτώσεις.

Επιπτώσεις:

- Διακοπή επικοινωνίας μεταξύ edge και fog κόμβων
- Υποβάθμιση διαθεσιμότητας
- Απώλεια real-time δεδομένων

Selective Jamming:

Πιο εξελιγμένη μορφή όπου ο επιτιθέμενος στοχεύει συγκεκριμένα πακέτα (π.χ. control messages) αντί για ολόκληρο το κανάλι.

Επιπτώσεις:

- Στοχευμένη αποσταθεροποίηση
- Δυσκολία εντοπισμού της επίθεσης

Στα fog περιβάλλοντα, οι επιθέσεις αυτές είναι ιδιαίτερα κρίσιμες, καθώς τα συστήματα βασίζονται σε συνεχείς ροές δεδομένων χαμηλής καθυστέρησης (low-latency data streams). Η παραποίηση, καθυστέρηση ή παρεμπόδιση αυτών των ροών μπορεί να επηρεάσει άμεσα τη διαθεσιμότητα, την ακεραιότητα και την αξιοπιστία των παρεχόμενων υπηρεσιών, ιδίως σε εφαρμογές βιομηχανικής αυτοματοποίησης, υγείας ή έξυπνων υποδομών.

Αντίστοιχα, στο edge οι επιπτώσεις μπορεί να είναι ακόμη πιο άμεσες λόγω εγγύτητας στον φυσικό κόσμο, οδηγώντας (σε κρίσιμες εφαρμογές) όχι μόνο σε λειτουργική αστοχία αλλά και σε οικονομικές απώλειες, φυσική βλάβη εξοπλισμού ή κίνδυνο για την ανθρώπινη ασφάλεια [17].

4.1.2.5 Επιθέσεις Πλευρικού Καναλιου & Ανάλυσης Κίνησης

Πέρα από τις κλασικές δικτυακές επιθέσεις, σε περιβάλλοντα fog και edge computing εμφανίζονται και επιθέσεις πλευρικού καναλιού (side-channel attacks, κατά τις οποίες ο επιτιθέμενος δεν χρειάζεται απαραίτητα να παραβιάσει άμεσα το περιεχόμενο της επικοινωνίας ή τον κύριο μηχανισμό προστασίας του συστήματος. Αντίθετα, αξιοποιεί έμμεσες πηγές πληροφορίας, όπως χρονισμούς εκτέλεσης, μοτίβα κίνησης δικτύου, κατανάλωση πόρων, ηλεκτρομαγνητικές ή ακουστικές εκπομπές, καθώς και κοινόχρηστους υπολογιστικούς πόρους, προκειμένου να εξαγάγει κρίσιμα συμπεράσματα για τη λειτουργία του συστήματος ή ακόμη και για ευαίσθητα μυστικά, όπως κλειδιά και διαπιστευτήρια.

Η κατηγορία αυτή δεν περιορίζεται μόνο στην ανάλυση κίνησης (traffic analysis), αλλά περιλαμβάνει περισσότερες μορφές επιθέσεων, οι οποίες αξιοποιούν διαφορετικά κανάλια διαρροής:

(α) Traffic Analysis:

Σε αυτή τη μορφή επίθεσης, ο επιτιθέμενος δεν χρειάζεται να αποκρυπτογραφήσει το περιεχόμενο των πακέτων, αλλά αρκείται στην παρατήρηση μεταδεδομένων επικοινωνίας, όπως χρονισμοί, μεγέθη, συχνότητες πακέτων, περιοδικότητα ροών και μοτίβα ανταλλαγής δεδομένων. Μέσω αυτής της ανάλυσης μπορεί να συναγάγει πληροφορίες για τη λειτουργία συσκευών, για πρότυπα δραστηριότητας χρηστών ή για κρίσιμες λειτουργικές καταστάσεις του συστήματος. Σε fog και edge περιβάλλοντα, η απουσία μηχανισμών κάλυψης κίνησης (traffic obfuscation), τυχαιοποίησης χρονισμών ή παραγωγής τεχνητής κίνησης (dummy traffic) διευκολύνει τέτοιες επιθέσεις, οι οποίες επηρεάζουν τόσο την ιδιωτικότητα όσο και τη δυνατότητα στοχοποίησης κρίσιμων κόμβων, όπως edge gateways υψηλής αξίας.

(β) Επιθέσεις μέσω κοινόχρηστων πόρων (shared-resource side channels):

Σε εικονικοποιημένα ή πολυμισθωτικά (multi-tenant) περιβάλλοντα, side-channel επιθέσεις μπορούν να προκύψουν όταν δεν υπάρχει επαρκής απομόνωση μεταξύ εικονικών μηχανών, containers ή workloads που μοιράζονται τους ίδιους φυσικούς πόρους. Σε τέτοιες περιπτώσεις, ο επιτιθέμενος μπορεί να παρατηρεί μεταβολές σε κοινόχρηστους πόρους, όπως cache, CPU timing, memory buses ή I/O patterns, και να εξάγει πληροφορίες για τις δραστηριότητες άλλων workloads. Επιπλέον, όταν η απομόνωση είναι σοβαρά ανεπαρκής ή εσφαλμένα υλοποιημένη, ο κίνδυνος δεν περιορίζεται μόνο σε έμμεση διαρροή μέσω side channels, αλλά μπορεί να επεκταθεί και σε άμεση πρόσβαση σε δεδομένα άλλων εικονικών μηχανών, containers ή υπηρεσιών, γεγονός που συνιστά πλέον ευθεία παραβίαση της εμπιστευτικότητας. Αυτή η κατηγορία είναι ιδιαίτερα σημαντική σε fog κόμβους ή ισχυρότερους edge servers, όπου εκτελούνται πολλαπλές υπηρεσίες στο ίδιο υποκείμενο υλικό.

(γ) Φυσικά ή περιβαλλοντικά πλευρικά κανάλια (physical side channels):

Σε ορισμένες περιπτώσεις, η διαρροή πληροφορίας μπορεί να προκύψει από φυσικά σήματα που εκπέμπει ή παράγει η ίδια η συσκευή ή το περιβάλλον αλληλεπίδρασής της. Τέτοιες επιθέσεις μπορεί να βασίζονται σε ακουστικά σήματα, ηλεκτρομαγνητικές εκπομπές, κατανάλωση ισχύος ή και σε πρότυπα εισόδου χρήστη. Ενδεικτικά, έχουν περιγραφεί επιθέσεις όπου ο ήχος του πληκτρολογίου ή άλλες φυσικές εκπομπές χρησιμοποιούνται για την εξαγωγή κωδικών πρόσβασης ή ακόμη και ολόκληρων κρυπτογραφικών κλειδιών. Σε edge περιβάλλοντα, όπου οι συσκευές βρίσκονται κοντά στον φυσικό κόσμο και συχνά σε λιγότερο ελεγχόμενες τοποθεσίες, τέτοιοι κίνδυνοι μπορεί να είναι εντονότεροι.

4.1.2.6 Επιθέσεις σε Διαχειριστικές Διεπαφές και Μηχανισμούς Ελέγχου

Στο πλαίσιο αυτό, δεν μπορούν να αγνοηθούν οι επιθέσεις κατά των διεπαφών ελέγχου και διαχείρισης (management and control interfaces), οι οποίες ενδέχεται να αποτελέσουν «entry points» προς τους υπολογιστικούς, δικτυακούς και αποθηκευτικούς πόρους του συστήματος. Οι επιθέσεις περιλαμβάνουν από web-based SQL injection, μέχρι στοχευμένο credential stuffing ή brute-force σε APIs. Ιδιαίτερα επικίνδυνες είναι οι επιθέσεις supply chain, όπου τροποποιείται κακόβουλα το λογισμικό ή το configuration πριν φτάσει στους κόμβους.

Οι σχετικές επιθέσεις μπορούν να κατηγοριοποιηθούν ως εξής:

(α) Επιθέσεις σε επίπεδο εφαρμογής (Application-layer attacks):

Επιθέσεις όπως SQL injection, command injection ή cross-site scripting (XSS) στοχεύουν web-based διαχειριστικές κονσόλες, αξιοποιώντας αδυναμίες στην επικύρωση και επεξεργασία εισόδου. Το SQL injection μπορεί να οδηγήσει σε μη εξουσιοδοτημένη πρόσβαση ή τροποποίηση δεδομένων της βάσης, το command injection σε εκτέλεση αυθαίρετων εντολών στο λειτουργικό σύστημα, ενώ το XSS σε εκτέλεση κακόβουλου κώδικα στον φυλλομετρητή του διαχειριστή, με πιθανή υποκλοπή συνεδριών ή παραποίηση ενεργειών [5].

Επιπτώσεις:

- Παραβίαση εμπιστευτικότητας διαχειριστικών δεδομένων
- Τροποποίηση πολιτικών ασφαλείας
- Πλήρης ανάληψη ελέγχου κόμβου (node takeover)

(β) Credential-based attacks (Brute-force & Credential stuffing):

Οι επιθέσεις brute-force επιχειρούν συστηματική δοκιμή κωδικών πρόσβασης, ενώ το credential stuffing αξιοποιεί διαρρεύσαντα credentials από άλλα συστήματα. Σε περιβάλλοντα όπου δεν εφαρμόζεται multi-factor authentication ή rate limiting, οι επιθέσεις αυτές μπορεί να οδηγήσουν σε μη εξουσιοδοτημένη πρόσβαση σε control APIs ή dashboards.

Επιπτώσεις:

- Απόκτηση διαχειριστικών δικαιωμάτων
- Παραβίαση αρχών least privilege
- Εγκατάσταση κακόβουλων workloads
- Πλήρης ανάληψη ελέγχου κόμβου (node takeover)

(γ) Επιθέσεις Supply Chain:

Οι επιθέσεις αυτές δεν στοχεύουν απευθείας τον fog κόμβο, αλλά τα στοιχεία από τα οποία αυτός απαρτίζεται. Αυτό μπορεί να περιλαμβάνει:

- Κακόβουλη τροποποίηση container base images
- Εισαγωγή κακόβουλου κώδικα σε βιβλιοθήκες τρίτων (third-party dependencies)
- Παραποίηση configuration αρχείων πριν την ανάπτυξη (deployment)
- Μη υπογεγραμμένες ή αλλοιωμένες ενημερώσεις firmware

Εδώ, γίνεται εκμετάλλευση τρωτοτήτων σε στοιχεία του συστήματος του κόμβου που μπορούν να αφορούν είτε το τελικό λογισμικό που εγκαθίσταται σε αυτόν είτε επιμέρους συστατικά του (π.χ. libraries, runtime components, container images, orchestration manifests).

Επιπτώσεις:

- Ενσωματωμένη κακόβουλη λειτουργικότητα (backdoors)
- Μαζική παραβίαση πολλαπλών κόμβων (με την ίδια διαμόρφωση συστήματος)
- Μακροχρόνια και δυσδιάκριτη παρουσία επιτιθέμενου (persistent compromise)

Στα fog περιβάλλοντα, οι επιθέσεις supply chain είναι ιδιαίτερα επικίνδυνες λόγω της μαζικής και αυτοματοποιημένης ανάπτυξης (automated deployment) κόμβων. Μια κακόβουλη τροποποίηση σε ένα base image ή configuration

template μπορεί να αναπαραχθεί ταυτόχρονα σε μεγάλο αριθμό κόμβων, οδηγώντας σε συστημική παραβίαση.

4.1.2.7 Επιθέσεις στην Ακεραιότητα Υπολογισμών (Attacks on Computation Integrity)

Σε fog και ιδιαίτερα σε edge περιβάλλοντα, όπου εκτελούνται τοπικοί υπολογισμοί (π.χ. analytics/AI/ML) πριν τα δεδομένα προωθηθούν ανάντη, ο αντίπαλος μπορεί να στοχεύσει όχι μόνο την ακεραιότητα των πακέτων αλλά και την "ορθότητα" του αποτελέσματος. Επιθέσεις όπως adversarial inputs σε μοντέλα μηχανικής μάθησης ή χειραγώγησης εισροών μπορούν να οδηγήσουν σε συστηματικά σφάλματα στις αποφάσεις χωρίς εμφανή ίχνη παραβίασης. Αυτό καθιστά απαραίτητη την ύπαρξη μηχανισμών επικύρωσης/επανελέγχου αποτελεσμάτων (result verification), (π.χ. επανεκτέλεση κρίσιμων υπολογισμών σε δεύτερο κόμβο για διασταύρωση, χρήση checksums/hashes για την επαλήθευση ενδιάμεσων αποτελεσμάτων ή έλεγχος συνέπειας βάσει προκαθορισμένων κανόνων), οι οποίοι όμως πρέπει να είναι αποδοτικοί (ιδίως ενεργειακά) για να είναι εφαρμόσιμοι στις edge συσκευές [17].

4.1.2.8 Επιθέσεις Εμπιστοσύνης και Μηχανισμών Ταυτοποίησης (Sybil Attack)

Η επίθεση Sybil αφορά την κατάχρηση του μηχανισμού ταυτοποίησης σε κατανεμημένα περιβάλλοντα, όπου ένας επιτιθέμενος δημιουργεί ή ελέγχει πολλαπλές ψευδείς ταυτότητες κόμβων (identities) και τις εισάγει στο δίκτυο ως δήθεν ανεξάρτητους συμμετέχοντες. Σε fog και edge σενάρια, όπου οι κόμβοι μπορούν να εντάσσονται/αποχωρούν δυναμικά και συχνά δεν υφίσταται ενιαία κεντρική αρχή πιστοποίησης, η Sybil επίθεση μπορεί να επηρεάσει μηχανισμούς εμπιστοσύνης και συντονισμού (π.χ. reputation/trust scoring, διαδικασίες επιλογής γειτόνων, ανάθεση εργασιών/task offloading ή ακόμη και διαδικασίες επικύρωσης/consensus). Οι επιπτώσεις περιλαμβάνουν χειραγώγηση αποφάσεων κατανομής πόρων, προώθηση παραποιημένων δεδομένων από «φαινομενικά» πολλούς κόμβους, υποβάθμιση διαθεσιμότητας μέσω υπερφόρτωσης/αποσταθεροποίησης και γενικότερη διάβρωση της αξιοπιστίας του οικοσυστήματος.

4.1.2.9 Αλυσιδωτές και Συστημικές Επιπτώσεις Επιθέσεων (Cascade Effects and Systemic Impact)

Εν τέλει, οι αλυσιδωτές επιπτώσεις από την αποτυχία ενός κόμβου λόγω επίθεσης είναι πιθανές, αν και η αρχιτεκτονική fog υποτίθεται πως σχεδιάζεται ώστε να παρέχει ανοχή σε σφάλματα (fault tolerance) και αντοχή σε αποτυχίες (resilience). Εάν η τοπολογία του δικτύου δεν είναι ορθά σχεδιασμένη, εάν οι πολιτικές fallback και ανακατεύθυνσης φορτίου (load redistribution) είναι ανεπαρκείς ή εάν οι γειτονικοί κόμβοι λειτουργούν ήδη κοντά στα όρια της χωρητικότητάς τους, τότε η αποτυχία ενός κόμβου μπορεί να οδηγήσει σε υπερφόρτωση και σταδιακή αποσταθεροποίηση γειτονικών στοιχείων. Σε τέτοιες περιπτώσεις, η συνολική διαθεσιμότητα της υποδομής ενδέχεται να τεθεί σε κίνδυνο [2].

Στην αλυσιδωτή αυτή δυναμική συμβάλλει και η έλλειψη μηχανισμών διαχείρισης εμπιστοσύνης (trust management). Σε αποκεντρωμένα fog περιβάλλοντα, οι κόμβοι συχνά αλληλεπιδρούν δυναμικά χωρίς να υφίσταται ενιαίος, αυστηρός μηχανισμός αξιολόγησης της αξιοπιστίας τους. Εάν ένας παραβιασμένος κόμβος συνεχίσει να θεωρείται έμπιστος από τους γειτονικούς του, μπορεί να διαδώσει κακόβουλα δεδομένα, να προωθήσει παραποιημένες εντολές ή να επηρεάσει αλγορίθμους κατανομής φορτίου, επιτείνοντας τη διάδοση της αποσταθεροποίησης. Η απουσία δυναμικών μηχανισμών trust scoring, reputation systems ή συνεχούς επαλήθευσης ταυτότητας καθιστά το σύστημα πιο ευάλωτο σε τέτοιες συστημικές επιπτώσεις.

Παράλληλα, η ανθεκτικότητα μιας fog υποδομής δεν εξαρτάται μόνο από την ύπαρξη πλεονασμού (redundancy), αλλά και από την ικανότητα έγκαιρης ανίχνευσης και αναχαίτισης επιθέσεων. Εάν δεν εφαρμόζονται μηχανισμοί απομόνωσης παραβιασμένων κόμβων (node isolation), περιορισμού κυκλοφορίας (traffic throttling), ή δυναμικής επαναδιαμόρφωσης της τοπολογίας (dynamic reconfiguration), τότε οι επιπτώσεις μιας επίθεσης ενδέχεται να εξαπλωθούν σε πολλαπλά επίπεδα της αρχιτεκτονικής. Συνεπώς, η αντιμετώπιση των αλυσιδωτών επιπτώσεων προϋποθέτει όχι μόνο σχεδιασμό για ανοχή σε σφάλματα, αλλά και ενεργητικούς μηχανισμούς ανίχνευσης, περιορισμού και ανάκτησης (detection, containment, recovery), ώστε να αποτρέπεται η συστημική διάχυση της απειλής.

Συνοψίζοντας, τα ζητήματα ασφάλειας στο fog computing δεν αφορούν μόνο τη θεωρητική ύπαρξη επιθέσεων, αλλά πηγάζουν από βαθιά αρχιτεκτονικές αδυναμίες, σφάλματα σχεδίασης, αστοχίες υλοποίησης, λανθασμένες διαμορφώσεις λογισμικού και ελλείψεις σε πολιτικές ασφαλούς ανάπτυξης. Κατά συνέπεια, η αποτελεσματική άμυνα προϋποθέτει συνδυαστική προσέγγιση: σχεδίαση ανθεκτικών αρχιτεκτονικών, ασφαλή ανάπτυξη λογισμικού, εγκαθίδρυση και κατάλληλη διατήρηση μοντέλων εμπιστοσύνης (trust models), και διαρκή διαρκή διαχειριση ρίσκου. Οι πιθανές λύσεις για την κάλυψη αυτών των απαιτήσεων θα αναλυθούν στην Ενότητα 4.3 (λύσεις ανεξάρτητες του blockchain) & στο Κεφάλαιο 5 (λύσεις ειδικές ως προς την εφαρμογή του blockchain).

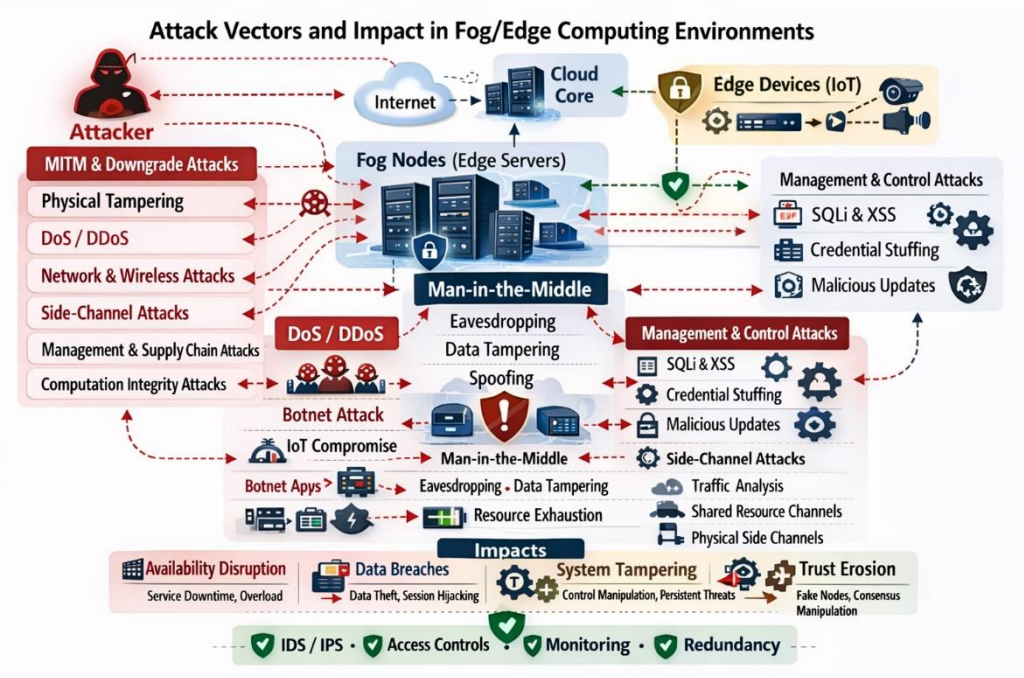
Πίνακας 6: Κατηγοριοποίηση Επιθέσεων σε Fog και Edge Περιβάλλοντα

Κατηγορία	Είδος Επίθεσης	Υπο-είδη	Στόχος	Επιπτώσεις (CIA)
	Man-in-the-Middle (MITM)	Eavesdropping	Κανάλι επικοινωνίας	Παραβίαση Εμπιστευτικότητας
		Active MITM / Data Tampering	Μεταφερόμενα δεδομένα / control traffic	Παραποίηση (Integrity)

Επιθέσεις Παρεμβολής Επικοινωνίας		Downgrade Attack	Πρωτόκολλο TLS/DTLS ή αλγόριθμοι	Αποδυνάμωση Κρυπτογράφησης
		Spoofing / Certificate Injection	Ταυτότητα κόμβου	Session Hijacking
Επιθέσεις Διαθεσιμότητας	DoS	Flooding	Fog Node	Υποβάθμιση Διαθεσιμότητας
	DDoS (Multi-stage)	IoT Botnet-based	Fog / Cloud	Παράλυση Υπηρεσιών, απώλεια διαθεσιμότητας
	IoT Compromise	Brute-force / Firmware exploit / Injection	IoT Device	Δημιουργία Botnet
	Resource Exhaustion / Battery-Drain	Compute amplification, connection amplification, τεχνητά αυξημένο φορτίο	Edge node resources / resource-constrained fog nodes	Υποβάθμιση διαθεσιμότητας, εξάντληση ενέργειας / QoS degradation
Δικτυακές Επιθέσεις και Επιθέσεις σε Ασύρματα Μέσα Μετάδοσης	Replay Attack	Packet Replay	Control Messages	Παραβίαση ακεραιότητας, εκτέλεση παλαιών εντολών
	Packet Injection	Forged Packets	Sensor/Control Traffic	Παραβίαση ακεραιότητας, ενδεχομένως και διαθεσιμότητας
	Reflection Attack	Reflection / amplification	Gateways / control infrastructure / intermediate nodes	Υποβάθμιση διαθεσιμότητας
	Jamming	Full-channel Jamming	Wireless Channel	Απώλεια Επικοινωνίας
	Selective Jamming	Control Packet Targeting	Specific Flows	Στοχευμένη Αποσταθεροποίηση
Επιθέσεις Πλευρικού Καναλιού και	Traffic Analysis	Metadata correlation (timing / size / frequency / periodicity)	Communication patterns	Παραβίαση εμπιστευτικότητας μεταδεδομένων, στοχοποίηση κόμβων

Ανάλυσης Κίνησης	Shared-resource Side-Channel Attacks	Cache timing, CPU timing, memory bus / I/O observation	Multi-tenant fog nodes / edge servers	Παραβίαση εμπιστευτικότητας, ενδεχομένως και άμεση διαρροή δεδομένων σε περιπτώσεις ανεπαρκούς απομόνωσης
	Physical Side-Channel Attacks	Acoustic, electromagnetic, power-analysis, environmental leakage	Edge devices / physically exposed systems	Παραβίαση εμπιστευτικότητας, εξαγωγή κλειδιών / διαπιστευτηρίων
Επιθέσεις σε Διαχειριστικές Διεπαφές και Μηχανισμούς Ελέγχου	**Application-Layer Επιθέσεις**	SQL Injection	Web Console	Node Takeover
		Command Injection	REST API	Εκτέλεση Κακόβουλου Κώδικα
		XSS	Web UI	Credential Theft
	Credential-based Επιθέσεις	Brute-force	Admin APIs	Μη εξουσιοδοτημένη κλιμάκωση προνομίων
		Credential Stuffing	Control Panels	Unauthorized Access
	Supply Chain Επιθέσεις	Malicious Base Image	Runtime	Εγκατάσταση κρυφής κακόβουλης λειτουργικότητας
		Compromised Library	Application Stack	Persistent Compromise
		Malicious Firmware Update	Device Firmware	System-wide Infection
Trust-based Επιθέσεις	Rogue Node	Node Impersonation	Distributed Trust	Διάδοση Κακόβουλων Δεδομένων
	Byzantine Behaviour	Malicious Cooperation	Fog Cluster	Αποσταθεροποίηση Αλγορίθμων
	Sybil Attack	Identity Multiplication	Distributed Trust / Reputation / Coordination	Αποσταθεροποίηση Εμπιστοσύνης (Integrity) / Υποβάθμιση Διαθεσιμότητας (Availability)

Συστημικές Επιθέσεις	Cascading Failure Exploitation	Overload Propagation μετά από συμβιβασμό ή αποτυχία κόμβου	Fog Topology	Συστημική υποβάθμιση ή απώλεια διαθεσιμότητας
	Failure Containment Bypass	No Isolation	Distributed System	Μαζική Διάδοση Επιπτώσεων
Επιθέσεις Φυσικής Πρόσβασης	Physical Tampering / Device Capture	Hardware tampering, key extraction, memory dump, firmware replacement, debug via UART/JTAG	Edge device / Fog node in public sites	Παραβίαση Ακεραιότητας/ Εμπιστευτικότητας/ Διαθεσιμότητας
Επιθέσεις Ακεραιότητας Υπολογισμών	Adversarial Inputs	ML evasion / input manipulation	Edge/Fog analytics	Λανθασμένες αποφάσεις (Integrity)



Εικόνα 10: Επιθέσεις σε fog/edge περιβάλλοντα

4.2. Ζητήματα Ιδιωτικότητας

Η ιδιωτικότητα στο πλαίσιο του fog computing συνιστά μια σύνθετη και πολυδιάστατη πρόκληση. Ο όρος ιδιωτικότητα, σε τεχνικά περιβάλλοντα πληροφορικής, αναφέρεται στην ικανότητα ελέγχου της πρόσβασης, χρήσης και επεξεργασίας των προσωπικών ή ευαίσθητων δεδομένων από τους ίδιους τους κατόχους τους. Στο fog computing, όπου οι πληροφορίες συλλέγονται, μεταδίδονται και επεξεργάζονται σε περιφερειακά επίπεδα του δικτύου, η διατήρηση αυτής της ιδιότητας συχνά καθίσταται δυσχερής. Αντίστοιχα, στο edge computing—όπου η επεξεργασία και η αποθήκευση μεταφέρονται ακόμη πιο κοντά στην πηγή (τελικές συσκευές, gateways, micro-nodes)—η ιδιωτικότητα καθίσταται εξίσου, και συχνά περισσότερο, ευάλωτη λόγω της μεγαλύτερης διασποράς κόμβων, της εναλλαγής τοπολογίας και της απουσίας ενιαίας εποπτείας [17].

Στα περιβάλλοντα fog και edge computing, η ιδιωτικότητα δεν περιορίζεται μόνο στην προστασία του περιεχομένου των δεδομένων, αλλά εκτείνεται σε επιμέρους διαστάσεις που επηρεάζονται από τη συλλογή, επεξεργασία και διακίνηση πληροφορίας. Ειδικότερα, μπορούν να διακριθούν τέσσερα βασικά είδη ιδιωτικότητας: (α) *η ιδιωτικότητα δεδομένων (data privacy)*, η οποία αφορά την προστασία του ίδιου του περιεχομένου των προσωπικών ή ευαίσθητων δεδομένων από μη εξουσιοδοτημένη πρόσβαση ή αποκάλυψη· (β) *η ιδιωτικότητα χρήσης ή συμπεριφοράς (usage/privacy of behavior)*, η οποία συνδέεται με την εξαγωγή συμπερασμάτων για τις συνήθειες, τις δραστηριότητες ή την κατάσταση ενός χρήστη μέσω της ανάλυσης προτύπων επικοινωνίας, τηλεμετρίας ή αλληλεπίδρασης με το σύστημα· (γ) *η ιδιωτικότητα ταυτότητας (identity privacy)*, η οποία αφορά την αποτροπή άμεσης ή έμμεσης ταυτοποίησης του υποκειμένου των δεδομένων, ακόμη και όταν χρησιμοποιούνται ψευδωνυμοποιημένα ή μερικώς ανωνυμοποιημένα δεδομένα· και (δ) *η ιδιωτικότητα τοποθεσίας (location privacy)*, η οποία σχετίζεται με την προστασία πληροφοριών που αποκαλύπτουν τη γεωγραφική θέση, τις μετακινήσεις ή τη χωρική συσχέτιση χρηστών και συσκευών. Οι τέσσερις αυτές διαστάσεις είναι ιδιαίτερα κρίσιμες στα fog/edge περιβάλλοντα, καθώς η εγγύτητα στην πηγή παραγωγής των δεδομένων, η κατανεμημένη

επεξεργασία και η έντονη εξάρτηση από συμφραζόμενα (context) αυξάνουν τον κίνδυνο αποκάλυψης όχι μόνο του “τι” δεδομένα παράγονται, αλλά και του “ποιος”, “πού” και “πώς” δρα μέσα στο σύστημα.

Καθώς τα δεδομένα συλλέγονται από τερματικές συσκευές, όπως αισθητήρες, έξυπνες συσκευές και υποδομές Internet of Things (IoT), και υποβάλλονται σε προκαταρκτική επεξεργασία πλησίον του σημείου δημιουργίας τους, αυξάνεται ο κίνδυνος έκθεσης προσωπικών ή ευαίσθητων πληροφοριών. Τα δεδομένα αυτά μπορεί να περιλαμβάνουν, μεταξύ άλλων, στοιχεία τοποθεσίας, δεδομένα υγείας ή συμπεριφορικά μοτίβα χρηστών, των οποίων η διαρροή θα μπορούσε να οδηγήσει όχι μόνο σε σοβαρές παραβιάσεις ιδιωτικότητας αλλά και σε πιθανή οικονομική ζημία ή νομική έκθεση, όπως η επιβολή υπέρογκων προστίμων λόγω μη συμμόρφωσης με τον GDPR ή άλλες ρυθμιστικές απαιτήσεις [2]. Στο edge, οι τύποι δεδομένων είναι συχνά ακόμη πιο “πλούσιοι” και ευαίσθητοι (π.χ. βιομετρικά σήματα, τηλεμετρία 5G/IoT, δεδομένα οικιακών/αστικών υποδομών), ενώ η τοπική προσωρινή αποθήκευση (caching) ή η διατήρηση logs σε συσκευές μπορεί να αυξήσει τον κίνδυνο άμεσης έκθεσης σε περίπτωση παραβίασης [17].

Στη συνέχεια, τα ζητήματα ιδιωτικότητας στο fog computing διακρίνονται σε (α) τρωτότητες που αυξάνουν την έκθεση ή μειώνουν τον έλεγχο επί των δεδομένων και (β) επιθέσεις/τεχνικές εκμετάλλευσης, οι οποίες αξιοποιούν αυτές τις αδυναμίες για την εξαγωγή ή αποκάλυψη ευαίσθητης πληροφορίας. Για λόγους συστηματικής ανάλυσης, οι βασικές αυτές κατηγορίες ζητημάτων ιδιωτικότητας, τα υπο-είδη τους, οι στόχοι τους και οι κύριες επιπτώσεις τους ως προς την έκθεση, την αποκάλυψη και τον έλεγχο ευαίσθητων δεδομένων παρουσιάζονται συνοπτικά στον **Error! Reference source not found.**.

4.2.1 Τρωτότητες Ιδιωτικότητας (Privacy vulnerabilities)

Αδιαφάνεια διαδρομών δεδομένων (data path opacity)

Ένα από τα βασικά προβλήματα συνδέεται με τη δυσκολία ελέγχου της διαδρομής που ακολουθούν τα δεδομένα εντός του κατανεμημένου περιβάλλοντος ομίχλης. Εξαιτίας της δυναμικής ανάθεσης φορτίου και της συμμετοχής διαφορετικών διοικητικών φορέων ή ιδιοκτητών υποδομής στους κόμβους fog, τα δεδομένα μπορεί να διέλθουν από πολλαπλούς ενδιάμεσους σταθμούς, χωρίς ο τελικός χρήστης ή ο πάροχος υπηρεσίας να έχει πλήρη επίγνωση της πορείας τους. Αυτό το χαρακτηριστικό αυξάνει τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης από μη έμπιστα μέρη, ιδιαίτερα εάν δεν έχουν εφαρμοστεί επαρκείς μηχανισμοί κρυπτογράφησης και ελέγχου πρόσβασης [2]. Αντίστοιχα, στο edge η “αδιαφάνεια διαδρομών” ενισχύεται από το ότι τα δεδομένα μπορεί να παραμείνουν τοπικά, να περάσουν από πύλες (gateways) ή να προωθηθούν επιλεκτικά προς fog/cloud ανάλογα με την κατάσταση του δικτύου και τις πολιτικές offloading, καθιστώντας δυσκολότερο τον καθορισμό του “πού βρίσκονται” και “ποιος τα επεξεργάζεται” σε κάθε χρονική στιγμή με αποτέλεσμα να υπάρχουν νομικά ζητήματα όταν τα δεδομένα καταλήγουν σε μια απαγορευμένη τοποθεσία [17].

Ετερογένεια συσκευών και διοικητικών φορέων

Διευρύνοντας τη προηγούμενη σκέψη, η ετερογένεια των συσκευών και των πλατφορμών που συνδέονται σε ένα fog computing περιβάλλον καθιστά δυσχερή την εφαρμογή ενιαίων πολιτικών προστασίας ιδιωτικότητας. Οι κόμβοι ομίχλης ενδέχεται να ανήκουν σε διαφορετικούς οργανισμούς ή παρόχους, οι οποίοι υιοθετούν διαφορετικά επίπεδα συμμόρφωσης με τα πρότυπα προστασίας προσωπικών δεδομένων. Αυτή η πολυπλοκότητα μπορεί να οδηγήσει σε ασυνέπειες ως προς τη διαχείριση των δικαιωμάτων πρόσβασης και τη διασφάλιση της ανωνυμοποίησης των δεδομένων [2]. Στο edge, το ίδιο πρόβλημα εμφανίζεται εντονότερα, επειδή οι κόμβοι/συσκευές διαφέρουν ακόμη περισσότερο ως προς λειτουργικά, firmware, πολιτικές ενημέρωσης και "ιδιοκτησιακή ευθύνη" (end-users, επιχειρήσεις, πάροχοι υποδομών, κατασκευαστές), γεγονός που δυσχεραίνει τη συνεπή επιβολή πολιτικών συγκατάθεσης, ελαχιστοποίησης και περιορισμού σκοπού [17].

Διαρροή μεταδεδομένων και μοτίβων επικοινωνίας

Ένα ακόμη κρίσιμο σημείο αφορά την ύπαρξη τρωτοτήτων που επιτρέπουν διαρροή μεταδεδομένων και συσχετισμούς επικοινωνίας, τόσο σε fog όσο και σε edge περιβάλλοντα. Συγκεκριμένα, η μη απόκρυψη χαρακτηριστικών της επικοινωνίας — όπως ο χρονισμός αποστολής/λήψης, το μέγεθος και η συχνότητα πακέτων, καθώς και η ύπαρξη προβλέψιμων ή περιοδικών ροών δεδομένων — δημιουργεί συνθήκες όπου, ακόμη και με κρυπτογράφηση περιεχομένου, παραμένει εκτεθειμένη η πληροφορία που αποτυπώνεται στα μοτίβα κίνησης. Επιπλέον, η απουσία μηχανισμών κάλυψης κίνησης (traffic obfuscation), τυχαιοποίησης χρονισμών ή δημιουργίας "dummy traffic" αφήνει την επικοινωνία ευάλωτη σε ανάλυση και συσχετισμούς [2]. Στο edge, όπου πολλές συσκευές επικοινωνούν ασύρματα και παράγουν περιοδική τηλεμετρία, η προβλεψιμότητα αυτή μπορεί να αποκαλύψει άμεσα συνήθειες χρήσης ή καταστάσεις λειτουργίας (π.χ. παρουσία/απουσία χρήστη, μοτίβα υγείας), ακόμη και χωρίς πρόσβαση στο περιεχόμενο [17].

Κίνδυνος φυσικής παραβίασης κόμβων

Στο ίδιο πλαίσιο, η τοποθεσία των κόμβων fog σε γεωγραφικά διασκορπισμένες περιοχές και η πιθανότητα φυσικής πρόσβασης σε αυτούς εντείνουν τον κίνδυνο φυσικής παραβίασης, όπως της εξαγωγής δεδομένων απευθείας από τα αποθηκευτικά μέσα, κλείδωμα δεδομένων, απώλεια ελέγχου, καταστροφή δεδομένων, δραστηριότητας ή την ύπαρξη συνεχούς παρακολούθησης υγειονομικών μετρήσεων, επανεκκίνησης σε μη ασφαλές mode ή εγκατάστασης malware μέσω φυσικής διεπαφής. Ειδικά σε περιπτώσεις όπου οι κόμβοι είναι εγκατεστημένοι σε δημόσιους χώρους ή απομακρυσμένες τοποθεσίες, ο έλεγχος της φυσικής ασφάλειας καθίσταται εξαιρετικά δυσχερής, δημιουργώντας έτσι μια ακόμη αδυναμία ως προς την προστασία της ιδιωτικότητας των πληροφοριών. Σε αντίθεση, οι κόμβοι σε ιδιωτικές εγκαταστάσεις μπορούν να εποπτεύονται και να προστατεύονται φυσικά, μειώνοντας αυτόν τον κίνδυνο [2]. Στο edge ο κίνδυνος φυσικής πρόσβασης είναι συχνά μεγαλύτερος, καθώς πολλές συσκευές βρίσκονται σε οικιακό/αστικό/βιομηχανικό χώρο χωρίς συνεχή επιτήρηση, ενώ η τοπική

αποθήκευση (buffers, caches, logs) μπορεί να περιέχει προσωπικά δεδομένα ή παράγωγα (inferences) έτοιμα προς εξαγωγή [17].

Εμπλοκή τρίτων παρόχων και ανάγκη μοντέλων εμπιστοσύνης

Ένα περαιτέρω σημείο που χρήζει αναφοράς αφορά την επεξεργασία δεδομένων από τρίτους παρόχους υπηρεσιών (third-party service providers), οι οποίοι ενδέχεται να αναλάβουν συγκεκριμένες λειτουργίες στο πλαίσιο του fog computing. Οι πάροχοι αυτοί μπορεί να είναι είτε φυσικοί (infrastructure providers) είτε λογικοί (service ή analytics providers) και συχνά δεν ανήκουν στο ίδιο οργανωτικό σχήμα με τον πάροχο της υπηρεσίας. Σε τέτοιες περιπτώσεις, οι χρήστες καλούνται να εμπιστευτούν εξωτερικές οντότητες για τη διαχείριση των δεδομένων τους, γεγονός που εισάγει πρόσθετους κινδύνους παραβίασης της ιδιωτικότητας, ιδίως όταν απουσιάζουν αυστηρές συμβατικές διασφαλίσεις ή σαφείς κανονιστικές ρυθμίσεις. Στο σημείο αυτό αναδεικνύεται και η ανάγκη ενός σαφούς μοντέλου εμπιστοσύνης (trust model), δηλαδή ο καθορισμός του “ποιος εμπιστεύεται ποιον” και υπό ποιες προϋποθέσεις (π.χ. πλήρης εμπιστοσύνη, μερική/υπό όρους εμπιστοσύνη ή μηδενική εμπιστοσύνη). Σε περιβάλλοντα όπου εμπλέκονται τρίτοι πάροχοι, η εμπιστοσύνη δεν μπορεί να θεωρείται δεδομένη και πρέπει να υποστηρίζεται είτε οργανωτικά (SLA/ρήτρες, συμμόρφωση) είτε τεχνικά (ισχυρός έλεγχος πρόσβασης, καταγραφή/ιχνηλασιμότητα, κρυπτογράφηση, attestation), ώστε να περιορίζεται η έκθεση των δεδομένων σε μη έμπιστα μέρη [2]. Στο edge η εμπλοκή τρίτων είναι επίσης συχνή (π.χ. πάροχοι διαχείρισης edge nodes, πλατφόρμες analytics, vendors συσκευών), ενώ ανακύπτουν εντονότερα ζητήματα διαφάνειας και συγκατάθεσης, καθώς ο τελικός χρήστης μπορεί να μην γνωρίζει ότι δεδομένα υποβάλλονται σε επεξεργασία από συγκεκριμένη εξωτερική οντότητα ή ότι διαμοιράζονται πέραν του “τοπικού” περιβάλλοντος [17].

Περιορισμοί ανωνυμοποίησης και επαναταυτοποίηση

Η ανωνυμοποίηση των δεδομένων αποτελεί μια συχνά προτεινόμενη πρακτική για τον μετριασμό των κινδύνων ιδιωτικότητας στο fog computing, πλην όμως, η εφαρμογή της δεν είναι πάντοτε εφικτή. Πέρα από την πιθανότητα επαναταυτοποίησης μέσω συσχετισμών, η εφαρμογή της ενδέχεται να αποτύχει για δύο κρίσιμους λόγους:

- **(α) Αδυναμία διάκρισης ευαίσθητων δεδομένων**: Σε αρκετές περιπτώσεις, τα δεδομένα δεν συνοδεύονται από κατάλληλη σημασιολογία ή μεταδεδομένα (metadata), με αποτέλεσμα ο επεξεργαστής (των δεδομένων) να μην είναι σε θέση να γνωρίζει ποια πεδία είναι κρίσιμα ή όχι. Το πρόβλημα εμφανίζεται τόσο σε ημι-δομημένα δεδομένα (π.χ. JSON/XML με δυναμικά πεδία), όπου η απουσία σταθερού σχήματος δυσχεραίνει την ταξινόμηση, όσο και –σε ακόμη μεγαλύτερο βαθμό– σε αδόμητα δεδομένα (π.χ. κείμενο, εικόνες, βίντεο), όπου η ευαισθησία δεν είναι εγγενώς συνδεδεμένη με συγκεκριμένα πεδία αλλά εντοπίζεται στο ίδιο το περιεχόμενο. Σε τέτοιες περιπτώσεις απαιτούνται πρόσθετοι μηχανισμοί ταξινόμησης και ανάλυσης περιεχομένου, ώστε να εφαρμοστούν ορθά πολιτικές προστασίας.

• **(β) Απώλεια ιδιοκτησίας δεδομένων**: Σε δυναμικά περιβάλλοντα όπως το fog, η επαναλαμβανόμενη επεξεργασία, μετατροπή και διακίνηση δεδομένων μπορεί να οδηγήσει στην αποσύνδεσή τους από τον αρχικό κάτοχο. Αυτό σημαίνει πως οι τελικοί χρήστες ίσως μην έχουν πλέον έλεγχο ή δυνατότητα εντοπισμού των δεδομένων τους, ιδιαίτερα όταν οι κόμβοι διαγράφουν καταχωρήσεις (logs), αλλάζουν μορφή ή προωθούν δεδομένα σε opaque layers.[14]

Τα προαναφερόμενα ζητήματα ιδιωτικότητας ισχύουν και στο edge, όπου τα δεδομένα μπορεί να παραμένουν σε τοπικές συσκευές ή να συντίθενται/συμπυκνώνονται σε "παράγωγα" (features, summaries), τα οποία παρότι φαίνονται μη-αναγνωρίσιμα, μπορούν να επιτρέψουν επαναταυτοποίηση μέσω συσχέτισης με άλλες πηγές [17].

Δυσκολίες εφαρμογής διαφορικής ιδιωτικότητας

Σε πολλές περιπτώσεις, τα δεδομένα που συλλέγονται περιλαμβάνουν οιωνεί-αναγνωρίσιμα χαρακτηριστικά που, ακόμα και αν διαγραφούν τα απευθείας αναγνωρίσιμα στοιχεία, δύνανται να επιτρέψουν την εκ νέου ταυτοποίηση των χρηστών μέσω τεχνικών συσχέτισης (re-identification techniques). Το γεγονός αυτό καθιστά αναγκαία τη χρήση πιο εξελιγμένων τεχνικών προστασίας, όπως η διαφορική ιδιωτικότητα (differential privacy), αν και η ενσωμάτωσή τους στις κατανεμημένες υποδομές ομίχλης παραμένει τεχνικά και λειτουργικά περίπλοκη [2]. Η πολυπλοκότητα αυτή οφείλεται στη κατανεμημένη φύση της αρχιτεκτονικής fog, όπου η διαχείριση του συνολικού privacy budget πρέπει να συντονίζεται μεταξύ πολλαπλών κόμβων, καθώς και στους περιορισμένους υπολογιστικούς πόρους και στις απαιτήσεις χαμηλής καθυστέρησης. Επιπλέον, μια πλημμελής ή αποσπασματική υλοποίηση των μηχανισμών διαφορικής ιδιωτικότητας ενδέχεται να οδηγήσει είτε σε ανεπαρκή προστασία (δημιουργώντας ψευδή αίσθηση ιδιωτικότητας) είτε σε σημαντική υποβάθμιση της χρησιμότητας των δεδομένων. Στο edge, οι περιορισμένοι πόροι (υπολογιστικοί/ενεργειακοί) μπορεί να οδηγήσουν σε "εκπτώσεις" στα τεχνικά μέτρα προστασίας (π.χ. απλουστευμένη κρυπτογράφηση, ασθενέστερη διαχείριση κλειδιών ή μη ενεργοποίηση ισχυρών μηχανισμών) με αποτέλεσμα αυξημένη έκθεση των δεδομένων σε κακόβουλη ανάγνωση ή μεταβολή [17].

Νομική και κανονιστική πολυπλοκότητα λόγω γεωγραφικής διασποράς

Τέλος, ιδιαίτερη τρωτότητα που αναδεικνύεται περισσότερο στο edge είναι η νομική/κανονιστική πολυπλοκότητα λόγω γεωγραφικής διασποράς και διακίνησης δεδομένων μεταξύ διαφορετικών δικαιοδοσιών, η οποία δημιουργεί ασάφειες ως προς το εφαρμοστέο δίκαιο, τη νομιμότητα επεξεργασίας και τη δυνατότητα επιβολής ποινών [17]. Το ίδιο μπορεί να εμφανιστεί και σε fog σενάρια πολλαπλών παρόχων/τοποθεσιών, αλλά στο edge εντείνεται από την "τοπικότητα" και την αδυναμία ενιαίας εποπτείας.

[14] Ενδιάμεσα τεχνολογικά επίπεδα σε μια κατανεμημένη αρχιτεκτονική (π.χ. middleware, virtualized ή third-party processing layers), στα οποία τα δεδομένα υφίστανται επεξεργασία ή μετασχηματισμό χωρίς διαφάνεια ως προς τις εσωτερικές λειτουργίες, περιορίζοντας τη δυνατότητα του αρχικού κατόχου να γνωρίζει, να ελέγχει ή να ιχνηλατεί τη μετέπειτα χρήση τους.

4.2.2 Επιθέσεις Παραβίασης Ιδιωτικότητας (Privacy Attacks)

Οι προαναφερόμενες τρωτότητες δεν αποτελούν αφηρημένες αδυναμίες, αλλά αξιοποιούνται ενεργά μέσω συγκεκριμένων επιθετικών τεχνικών. Ενδεικτικά, η ανάλυση κίνησης (traffic analysis) εκμεταλλεύεται τη διαρροή μεταδεδομένων και τα προβλέψιμα μοτίβα επικοινωνίας (χρονισμούς, μεγέθη, συχνότητες), ώστε να εξαχθούν συμπεράσματα σχετικά με τη δραστηριότητα των χρηστών ή τη λειτουργία των συσκευών, ακόμη και όταν το περιεχόμενο είναι κρυπτογραφημένο. Πρόκειται για επιθέσεις που εντάσσονται στην κατηγορία των πλευρικών καναλιών (side-channel attacks), καθώς δεν βασίζονται στην αποκρυπτογράφηση των δεδομένων, αλλά σε πληροφορίες που διαρρέουν έμμεσα από τη λειτουργία του συστήματος. Για παράδειγμα, η σταθερή και τακτική μετάδοση πακέτων από ένα smartwatch μπορεί να αποκαλύψει πρότυπα δραστηριότητας ή την ύπαρξη συνεχούς παρακολούθησης υγειονομικών μετρήσεων, χωρίς να παραβιαστεί άμεσα το περιεχόμενο [2]. Σε edge περιβάλλοντα, αντίστοιχες τεχνικές μπορούν να αξιοποιήσουν και λειτουργικές μετρήσεις (π.χ. patterns τηλεμετρίας, περιοδικότητα αισθητήρων) ώστε να εξαχθούν προφίλ χρήσης ή “καταστάσεις” του χρήστη/συστήματος [17].

Επιπλέον, επιθέσεις συσχέτισης και επαναταυτοποίησης (re-identification attacks) αξιοποιούν οιωνεί-αναγνωριστικά ή διασταυρούμενες πληροφορίες από διαφορετικές πηγές, ώστε να ανακτηθεί η ταυτότητα ενός χρήστη από δεδομένα που εμφανίζονται ως “ανώνυμα”. Αντίστοιχα, η συγκέντρωση και διασταύρωση δεδομένων (data aggregation) μπορεί να οδηγήσει στη δημιουργία λεπτομερών προφίλ χρήσης, ακυρώνοντας στην πράξη την προστασία που παρέχουν απλές μορφές ανωνυμοποίησης ή ψευδωνυμοποίησης [2]. Η πρακτική αυτή είναι ιδιαίτερα κρίσιμη στο edge, επειδή η συγχώνευση ετερογενών πηγών (τοποθεσία, βιομετρικά, συμπεριφορά, οικιακοί/βιομηχανικοί αισθητήρες) μπορεί να παράγει πολύ ακριβή προφίλ, ακόμη και αν κάθε ροή δεδομένων μεμονωμένα φαίνεται “ακίνδυνη” [17].

Τέλος, η φυσική παραβίαση κόμβων (π.χ. εξαγωγή δεδομένων από αποθηκευτικά μέσα ή τροποποίηση firmware) μπορεί να λειτουργήσει ως άμεσος μηχανισμός παραβίασης ιδιωτικότητας, ιδίως όταν οι κόμβοι είναι εγκατεστημένοι σε σημεία όπου η φυσική πρόσβαση δεν μπορεί να ελεγχθεί αποτελεσματικά [2]. Στο edge, η φυσική παραβίαση μπορεί να αφορά και “device capture” (κατάληψη/κλοπή συσκευής), οδηγώντας σε πρόσβαση σε τοπικά αποθηκευμένα δεδομένα, κλειδιά ή logs, ακόμη και χωρίς επιτυχή απομακρυσμένη εκμετάλλευση [17].

Επιπρόσθετα, σε fog/edge περιβάλλοντα όπου εκτελούνται αναλύσεις ή μοντέλα μηχανικής μάθησης πάνω σε ευαίσθητα δεδομένα, μπορούν να εμφανιστούν επιθέσεις εξαγωγής πληροφορίας από τα αποτελέσματα (inference attacks), όπου ο αντίπαλος αποκομίζει ιδιωτική πληροφορία από στατιστικά/εξόδους (π.χ. μέσω συσχέτισης, παρατηρούμενων μοτίβων ή/και διαδοχικών ερωτημάτων προς μια υπηρεσία).

Είναι σημαντικό να τονιστεί ότι πολλές επιθέσεις που παραβιάζουν ιδιότητες ασφάλειας (π.χ. εμπιστευτικότητα ή ακεραιότητα) συνεπάγονται ταυτόχρονα και παραβίαση της ιδιωτικότητας. Για παράδειγμα, μια επίθεση Man-in-the-Middle που εκμεταλλεύεται κακή διαχείριση πιστοποιητικών δεν πλήττει μόνο την εμπιστευτικότητα της επικοινωνίας, αλλά μπορεί να οδηγήσει και σε αποκάλυψη προσωπικών δεδομένων. Αντίστοιχα, επιθέσεις traffic analysis ή replay, παρότι εντάσσονται στις γενικές δικτυακές επιθέσεις, δύνανται να επιτρέψουν εξαγωγή προτύπων συμπεριφοράς χρηστών, επηρεάζοντας άμεσα την ιδιωτικότητα. Συνεπώς, η διάκριση μεταξύ τρωτοτήτων ασφάλειας και ιδιωτικότητας δεν είναι πάντοτε απόλυτη, καθώς συχνά υφίσταται σημαντική αλληλοεπικάλυψη.

Σημειώνεται ότι οι τρωτότητες ιδιωτικότητας της Ενότητας 4.2.1 δεν ταυτίζονται πλήρως με τις τρωτότητες ασφάλειας της Ενότητας 4.1.1. Σε αρκετές περιπτώσεις, οι τελευταίες λειτουργούν ως τεχνικοί ή οργανωτικοί παράγοντες που διευκολύνουν ή επιτείνουν την εκδήλωση των πρώτων. Για τον λόγο αυτό, ο Πίνακας 7 αποτυπώνει αφενός τις βασικές τρωτότητες ιδιωτικότητας που αναλύθηκαν στην Ενότητα 4.2.1 και αφετέρου τις συναφείς τρωτότητες ασφάλειας της Ενότητας 4.1.1 που συνδέονται με αυτές.

Πίνακας 7: Αντιστοίχιση Τρωτοτήτων Ιδιωτικότητας με Συναφείς Τρωτότητες Ασφάλειας, Επιθέσεις και Παραβιάσεις Ασφάλειας–Ιδιωτικότητας

Τρωτότητα ιδιωτικότητας (4.2.1)	Σχετικές τρωτότητες ασφάλειας από 4.1.1	Εκμεταλλευόμενη επίθεση / τεχνική	Παραβίαση ασφάλειας	Παραβίαση ιδιωτικότητας	Είδος ιδιωτικότητας που θίγεται
Αδιαφάνεια διαδρομών δεδομένων (data path opacity)	Τρωτότητες πρωτοκόλλων και ασφαλούς επικοινωνίας· τρωτότητες διαχειριστικών διεπαφών και μηχανισμών ελέγχου· τρωτότητες διαχείρισης εμπιστοσύνης και συνεργασίας κόμβων	MITM, eavesdropping, rogue intermediary routing, malicious task offloading	Εμπιστευτικότητα / Εξουσιοδότηση / Λογοδοσία	Μη διαφανής ή μη εξουσιοδοτημένη πρόσβαση και επεξεργασία δεδομένων κατά τη διαδρομή τους	Ιδιωτικότητα δεδομένων, ιδιωτικότητα τοποθεσίας, ιδιωτικότητα ταυτότητας, ενδεχομένως ιδιωτικότητα χρήσης/συμπεριφοράς
Ετερογένεια συσκευών και διοικητικών φορέων	Ετερογένεια συσκευών/κόμβων· τρωτότητες ενημερώσεων και κύκλου ζωής λογισμικού· οργανωτικές και ανθρωποκεντρικές τρωτότητες	Exploitation μη επιδιορθωμένων κόμβων, credential attacks, unauthorised processing / data sharing	Εξουσιοδότηση / Εμπιστευτικότητα / Λογοδοσία	Ασυνεπής επιβολή πολιτικών προστασίας, μη εξουσιοδοτημένη πρόσβαση ή επεξεργασία, ασαφής συγκατάθεση	Ιδιωτικότητα δεδομένων, ιδιωτικότητα ταυτότητας, ιδιωτικότητα τοποθεσίας, ιδιωτικότητα χρήσης/συμπεριφοράς
Διαρροή μεταδεδομένων και μοτίβων επικοινωνίας	Τρωτότητες πρωτοκόλλων και ασφαλούς επικοινωνίας· τρωτότητες εικονικοποίησης/δοχειοποίησης και απομόνωσης	Traffic analysis, side-channel correlation	Εμπιστευτικότητα	Εξαγωγή προτύπων δραστηριότητας, συσχέτιση επικοινωνιών, συναγωγή λειτουργικής κατάστασης ή παρουσίας χρήστη	Ιδιωτικότητα χρήσης/συμπεριφοράς, ιδιωτικότητα τοποθεσίας, ενδεχομένως ιδιωτικότητα ταυτότητας
Κίνδυνος φυσικής παραβίασης κόμβων	Τρωτότητες υλικού και φυσικής ασφάλειας· τρωτότητες ενημερώσεων και κύκλου ζωής λογισμικού	Physical tampering, device capture, data extraction, firmware tampering	Εμπιστευτικότητα / Ακεραιότητα / Διαθεσιμότητα	Ανάκτηση αποθηκευμένων προσωπικών δεδομένων, logs, κλειδιών ή παραγώγων πληροφορίας	Ιδιωτικότητα δεδομένων, ιδιωτικότητα ταυτότητας, ιδιωτικότητα χρήσης/συμπεριφοράς, ιδιωτικότητα τοποθεσίας
Εμπλοκή τρίτων παρόχων και ανάγκη μοντέλων εμπιστοσύνης	Τρωτότητες διαχείρισης εμπιστοσύνης και συνεργασίας κόμβων· οργανωτικές και ανθρωποκεντρικές τρωτότητες· τρωτότητες διαχειριστικών διεπαφών και μηχανισμών ελέγχου	Unauthorised processing / data sharing, rogue node participation, malicious task offloading	Εξουσιοδότηση / Λογοδοσία / Εμπιστευτικότητα	Επεξεργασία ή διαμοιρασμός δεδομένων από μη διαφανείς ή μη έμπιστες οντότητες χωρίς επαρκή ενημέρωση ή έγκυρη συγκατάθεση	Ιδιωτικότητα δεδομένων, ιδιωτικότητα ταυτότητας, ιδιωτικότητα τοποθεσίας, ιδιωτικότητα χρήσης/συμπεριφοράς

Περιορισμοί ανωνυμοποίησης και επαναταυτοποίηση	Έμμεση σχέση κυρίως με ετερογένεια συσκευών/κόμβων και οργανωτικές τρωτότητες	Re-identification attacks, data aggregation, inference attacks	Εμπιστευτικότητα / Ακεραιότητα πολιτικών προστασίας	Επαναταυτοποίηση χρήστη, απώλεια ελέγχου ή ιδιοκτησίας επί των δεδομένων	Ιδιωτικότητα ταυτότητας, ιδιωτικότητα δεδομένων, ιδιωτικότητα χρήσης/συμπεριφοράς, ενδεχομένως ιδιωτικότητα τοποθεσίας
Δυσκολίες εφαρμογής διαφορικής ιδιωτικότητας	Έμμεση σχέση κυρίως με ετερογένεια/περιορισμούς πόρων και κύκλο ζωής λογισμικού	Inference attacks, reconstruction, membership inference	Εμπιστευτικότητα	Ανεπαρκής προστασία μέσω πλημμελούς ρύθμισης privacy mechanisms ή υποβάθμιση χρησιμότητας που αποτρέπει ασφαλή υιοθέτηση	Ιδιωτικότητα δεδομένων, ιδιωτικότητα ταυτότητας, ιδιωτικότητα χρήσης/συμπεριφοράς, ενδεχομένως ιδιωτικότητα τοποθεσίας
Νομική και κανονιστική πολυπλοκότητα λόγω γεωγραφικής διασποράς	Οργανωτικές και ανθρωποκεντρικές τρωτότητες· τρωτότητες διαχείρισης εμπιστοσύνης και συνεργασίας κόμβων	Opaque routing, cross-border data transfer, unauthorised processing / retention	Λογοδοσία / Εξουσιοδότηση	Απώλεια ελέγχου επί των δεδομένων, μη νόμιμη επεξεργασία ή διαβίβαση, ασαφές καθεστώς συγκατάθεσης και ευθύνης	Ιδιωτικότητα δεδομένων, ιδιωτικότητα ταυτότητας, ιδιωτικότητα τοποθεσίας, ιδιωτικότητα χρήσης/συμπεριφοράς

Η αποτελεσματική προστασία της ιδιωτικότητας απαιτεί πολυεπίπεδες παρεμβάσεις, με τεχνικά, οργανωτικά και νομικά μέσα, που θα εξεταστούν διεξοδικά στα Κεφάλαια 5, 6, 7 και 8 της παρούσας εργασίας.

4.3. Σχετικές Προκλήσεις & Λύσεις στο Fog και στο Edge Computing

Η μελέτη των αρχιτεκτονικών fog computing ανέδειξε πληθώρα ζητημάτων που σχετίζονται με την ασφάλεια και την προστασία της ιδιωτικότητας των δεδομένων. Αντίστοιχα, η ανάλυση του edge computing επιβεβαιώνει ότι τα ίδια θεμελιώδη ζητήματα (CIA + ιδιωτικότητα) εμφανίζονται συχνά με μεγαλύτερη ένταση, λόγω της ακόμη μεγαλύτερης διασποράς, της φυσικής έκθεσης και των περιορισμένων πόρων των συσκευών. Η εξασφάλιση της ακεραιότητας, εμπιστευτικότητας, διαθεσιμότητας και ιδιωτικότητας καθίσταται κρίσιμη, καθώς χωρίς αυτές δεν είναι εφικτή η ευρεία αποδοχή και ενσωμάτωση των fog/edge υποδομών σε κατανεμημένα υπολογιστικά περιβάλλοντα [2]. Σε αντίθεση με το παραδοσιακό cloud, το fog computing εισάγει μεγαλύτερη πολυπλοκότητα λόγω της εγγύτητας στους τελικούς χρήστες και της παρουσίας πολλαπλών, ετερογενών και ενδεχομένως μη εμπιστευμένων κόμβων. Το ίδιο ισχύει και στο

edge, όπου οι κόμβοι συχνά βρίσκονται σε οικιακά/αστικά/βιομηχανικά περιβάλλοντα, με περιορισμένη εποπτεία και αυξημένη φυσική πρόσβαση.

Τα βασικά προβλήματα ασφάλειας εστιάζονται στην ανάγκη διασφάλισης των δεδομένων τόσο κατά τη μεταφορά όσο και κατά την επεξεργασία & αποθήκευσή τους σε κόμβους της ομίχλης. Αντίστοιχα, στο edge η προστασία πρέπει να εφαρμοστεί σε ακόμη περισσότερα σημεία (τερματικές συσκευές, gateways, μικρο-servers), αυξάνοντας την επιφάνεια επίθεσης και την ανάγκη για συνεπείς πολιτικές ασφάλειας σε μη ομοιογενείς πλατφόρμες [17]. Οι παραδοσιακές τεχνικές κρυπτογράφησης, όπως συμμετρική (AES), ασύμμετρη (RSA) ή υβριδικά σχήματα, συχνά αντιμετωπίζουν δυσκολίες εφαρμογής λόγω των περιορισμένων υπολογιστικών πόρων και της απαίτησης για χαμηλό χρόνο απόκρισης. Ιδιαίτερη πρόκληση αποτελεί η επίτευξη ασφαλούς επικοινωνίας χωρίς να διακυβεύεται η απόδοση, ιδίως σε εφαρμογές που απαιτούν πραγματικό χρόνο λειτουργίας [2].

Ωστόσο, τα υβριδικά κρυπτογραφικά σχήματα θεωρούνται πιο αποδοτική και πρακτική λύση για περιβάλλοντα fog, καθώς συνδυάζουν τα πλεονεκτήματα της συμμετρικής και της ασύμμετρης κρυπτογράφησης. Συγκεκριμένα, χρησιμοποιούν ασύμμετρη κρυπτογράφηση για την ασφαλή ανταλλαγή κλειδιών και την πιστοποίηση της αυθεντικότητας και ακεραιότητας των μηνυμάτων, ενώ στη συνέχεια αξιοποιούν συμμετρική κρυπτογράφηση για την ταχεία και ενεργειακά αποδοτική απόκρυψη του περιεχομένου των δεδομένων. Με τον τρόπο αυτό επιτυγχάνεται ισορροπία μεταξύ ασφάλειας και υπολογιστικής αποδοτικότητας, στοιχείο ιδιαίτερα κρίσιμο σε κατανεμημένα περιβάλλοντα με περιορισμένους πόρους [2]. Στο edge η ίδια λογική υλοποιείται συχνά με “ελαφρύτερες” παραλλαγές (π.χ. σύγχρονες ρυθμίσεις TLS/DTLS, ασφαλή cipher suites, session resumption), ώστε να περιορίζεται το κόστος χειραψίας/επανεγκαθίδρυσης συνόδων και να μην επιβαρύνεται το latency [17].

Επιπλέον, προτείνονται τεχνικές όπως η μερική κρυπτογράφηση (selective ή partial encryption), κατά την οποία κρυπτογραφούνται μόνο τα ευαίσθητα τμήματα των δεδομένων και όχι ολόκληρο το φορτίο πληροφορίας. Η προσέγγιση αυτή μειώνει το υπολογιστικό κόστος και την καθυστέρηση επεξεργασίας, διατηρώντας παράλληλα ικανοποιητικό επίπεδο προστασίας για κρίσιμες πληροφορίες. Παρότι τέτοιες τεχνικές βελτιώνουν την απόδοση, απαιτούν προσεκτικό σχεδιασμό ώστε να μην δημιουργούνται σημεία διαρροής μέσω των μη κρυπτογραφημένων τμημάτων των δεδομένων [2]. Συμπληρωματικά, ειδικά σε fog/edge τηλεμετρία, προτείνονται ρητά μηχανισμοί anti-replay (nonces, timestamps, sequence numbers) και αμοιβαία πιστοποίηση (mutual authentication), ώστε να μετριάζονται πιθανότητες spoofing/replay/packet-injection χωρίς υπερβολικό υπολογιστικό κόστος [17].

Παράλληλα, η αυθεντικοποίηση και η εξουσιοδότηση αποτελούν θεμελιώδεις προκλήσεις. Αν και έχουν εξεταστεί λύσεις που αφορούν ελαφρά συστήματα αυθεντικοποίησης, το πραγματικό πρόβλημα επεκτείνεται στην ανάγκη για πιο εκλεπτυσμένα και ευέλικτα μοντέλα ελέγχου πρόσβασης. Η βιβλιογραφία επισημαίνει ότι ο παραδοσιακός έλεγχος βάσει ρόλων (RBAC) δεν επαρκεί σε δυναμικά περιβάλλοντα όπως το fog, όπου η ταυτότητα, το πλαίσιο (context), η τοποθεσία ή ο χρόνος εκτέλεσης μπορεί να επηρεάζουν τους όρους

πρόσβασης. Για τον λόγο αυτό έχουν προταθεί εναλλακτικές προσεγγίσεις, όπως το ABAC (Attribute-Based Access Control), στο οποίο οι αποφάσεις πρόσβασης λαμβάνονται βάσει χαρακτηριστικών του χρήστη, του πόρου και του περιβάλλοντος, το PBAC (Policy-Based Access Control), όπου η πρόσβαση καθορίζεται από ρητές πολιτικές ασφαλείας που μπορούν να εκφράζουν σύνθετους κανόνες και περιορισμούς, καθώς και το context-aware RBAC ή CRBAC (Context-Aware Role-Based Access Control), το οποίο επεκτείνει το κλασικό RBAC ενσωματώνοντας συμφραζόμενες παραμέτρους, όπως η γεωγραφική θέση, η χρονική στιγμή, η κατάσταση της συσκευής ή το επίπεδο εμπιστοσύνης του κόμβου. Με τον τρόπο αυτό, η εξουσιοδότηση δεν βασίζεται μόνο στον στατικό ρόλο του υποκειμένου, αλλά και στις δυναμικές συνθήκες υπό τις οποίες ζητείται η πρόσβαση. Παρά το ενδιαφέρον που παρουσιάζουν οι προσεγγίσεις αυτές, δεν έχει ακόμη επιτευχθεί ευρεία εφαρμογή τους σε πραγματικές υποδομές fog [2]. Στο edge, η ανάγκη αυτή ενισχύεται από τη δυναμική ένταξη και αποχώρηση κόμβων και τη μη σταθερή τοπολογία, καθιστώντας κρίσιμες τις ασφαλείς διαδικασίες onboarding και την περιοδική επαλήθευση ταυτότητας και κατάστασης κόμβων (continuous verification, λογική zero trust) [17].

Οι λόγοι περιορισμένης υιοθέτησης σχετίζονται κυρίως με την αυξημένη πολυπλοκότητα διαχείρισης πολιτικών πρόσβασης, την ανάγκη συνεχούς συλλογής και επικύρωσης δυναμικών γνωρισμάτων (attributes), καθώς και το υπολογιστικό κόστος που συνεπάγεται η αξιολόγηση πολύπλοκων κανόνων σε περιβάλλοντα με περιορισμένους πόρους. Επιπλέον, η έλλειψη τυποποίησης και διαλειτουργικότητας μεταξύ ετερογενών συσκευών, καθώς και η απουσία ώριμων πλαισίων υλοποίησης σε πραγματικές υποδομές fog, καθιστούν την ευρεία εφαρμογή των μοντέλων αυτών ακόμη περιορισμένη [2]. Στην πράξη (fog/edge), η μείωση ρίσκου απαιτεί και “σκληρά” μέτρα υλοποίησης: ελάχιστα προνόμια (least privileges), δικτυακή τμηματοποίηση (network segmentation) και περιορισμό πλευρικής κίνησης επιτιθέμενου σε περίπτωση συμβιβασμού ενός κόμβου [17].

Ένα ιδιαίτερα κρίσιμο (και συχνά “πρακτικό”) σημείο στο edge—αλλά και σε fog κόμβους που εκθέτουν αντίστοιχες υπηρεσίες—είναι η σκλήρυνση των διαχειριστικών διεπαφών (management APIs/κονσόλες). Ενώ οι μηχανισμοί πολιτικών πρόσβασης είναι απαραίτητοι, η εμπειρική επίθεση συχνά αξιοποιεί ανοιχτές θύρες, προεπιλεγμένα διαπιστευτήρια, έλλειψη rate limiting και ανεπαρκές logging/audit trails, οδηγώντας σε takeover ή και remote code execution [17]. Ως λύσεις προτείνονται: απενεργοποίηση περιττών υπηρεσιών/θυρών, υποχρεωτική αλλαγή default credentials, ισχυρή αυθεντικοποίηση (όπου είναι εφικτό και MFA), rate limiting/lockout πολιτικές και συστηματική καταγραφή κρίσιμων ενεργειών για ιχνηλασιμότητα και απόκριση σε περιστατικά , καθώς και η υιοθέτηση τεχνικών ασφαλούς ανάπτυξης λογισμικού (secure software development practices), όπως ασφαλής επικύρωση εισόδου, ελαχιστοποίηση δικαιωμάτων, τακτικός έλεγχος κώδικα και δοκιμές ασφαλείας πριν από την παραγωγική διάθεση.

Στο πεδίο της ιδιωτικότητας, προβλήματα εντοπίζονται κυρίως στη διατήρηση της ανωνυμίας των χρηστών. Η χρήση τεχνικών ανωνυμοποίησης και ψευδωνυμοποίησης θεωρείται κρίσιμη, όμως η αποτελεσματικότητά τους

αμφισβητείται, ιδίως όταν υπάρχουν οιωνεί αναγνωριστικά που επιτρέπουν τον επαναπροσδιορισμό της ταυτότητας του χρήστη. Η απλή απόκρυψη ταυτοποιητικών στοιχείων δεν επαρκεί σε περιβάλλοντα όπου τα δεδομένα συσχετίζονται με τοποθεσία, χρόνο ή μοτίβα χρήσης. Σε αυτό το πλαίσιο, η χρήση τεχνικών data masking (Απόκρυψη δεδομένων) σε επίπεδο συλλογής ή αποθήκευσης όπως η μερική απόκρυψη πεδίων (partial masking) — όπου εμφανίζεται μόνο τμήμα της πληροφορίας — και η αντικατάσταση ή tokenization — όπου τα πραγματικά δεδομένα αντικαθίστανται από τεχνητές τιμές ίδιου μορφοτύπου — έχει προταθεί για την αποτροπή διαρροής κρίσιμων πληροφοριών, αν και απαιτείται περαιτέρω αξιολόγηση των περιπτώσεων όπου είναι κατάλληλη. Στο edge, οι ίδιες δυσκολίες εντείνονται λόγω ακόμη αυστηρότερων περιορισμών πόρων/ενέργειας, άρα απαιτείται προσεκτική επιλογή παραμέτρων και σαφής αξιολόγηση trade-off μεταξύ προστασίας και χρησιμότητας δεδομένων [17].

Η διαφορική ιδιωτικότητα (differential privacy), αν και θεωρείται θεωρητικά ισχυρή, συνοδεύεται από πρακτικά προβλήματα στην εφαρμογή της, κυρίως λόγω της ανάγκης για προσεκτική ρύθμιση παραμέτρων που επηρεάζουν το επίπεδο προστασίας (π.χ., η παράμετρος ε). Επιπλέον, η εισαγωγή θορύβου ενδέχεται να επηρεάζει αρνητικά την ακρίβεια των αποτελεσμάτων, ειδικά σε περιβάλλοντα με περιορισμένα δεδομένα. Παρά τις ερευνητικές προτάσεις που έχουν κατατεθεί, η διαφορική ιδιωτικότητα δεν έχει ακόμη καθιερωθεί ως πρακτικό εργαλείο στο fog computing, ενώ εναλλακτικές προσεγγίσεις, όπως η k-anonymity ή το secure multiparty computation, παραμένουν αντικείμενο μελέτης [2]. Στο edge, οι ίδιες δυσκολίες εντείνονται λόγω ακόμη αυστηρότερων περιορισμών πόρων/ενέργειας, άρα απαιτείται προσεκτική επιλογή παραμέτρων και σαφής αξιολόγηση trade-off μεταξύ προστασίας και χρησιμότητας δεδομένων [17]. Στην ίδια κατεύθυνση, έχουν προταθεί και επεκτάσεις όπως η l-diversity και η t-closeness, με στόχο να αντιμετωπιστούν αδυναμίες της k-anonymity ως προς την ομοιογένεια και τις επιθέσεις συσχέτισης, αν και και αυτές συνεπάγονται πρόσθετη πολυπλοκότητα και απώλεια χρησιμότητας.

Παράλληλα, ιδιαίτερο ενδιαφέρον παρουσιάζουν εξειδικευμένες μορφές κρυπτογράφησης που επιτρέπουν την επεξεργασία δεδομένων ενώ αυτά παραμένουν σε κρυπτογραφημένη μορφή. Χαρακτηριστικά παραδείγματα αποτελούν η ομομορφική κρυπτογράφηση (homomorphic encryption) και ο ασφαλής πολυμερής υπολογισμός (secure multiparty computation – SMPC), οι οποίες επιτρέπουν την εκτέλεση υπολογισμών χωρίς αποκάλυψη των αρχικών δεδομένων. Στις περιπτώσεις αυτές, τα δεδομένα παραμένουν κρυπτογραφημένα τόσο κατά τη μεταφορά όσο και κατά την επεξεργασία, μειώνοντας την ανάγκη εφαρμογής τεχνικών ανωνυμοποίησης ή data masking. Κατά συνέπεια, η ιδιωτικότητα διασφαλίζεται σε επίπεδο αρχιτεκτονικής σχεδιασμού, αν και το υψηλό υπολογιστικό κόστος και η πολυπλοκότητα υλοποίησης εξακολουθούν να περιορίζουν την ευρεία εφαρμογή των τεχνικών αυτών σε περιβάλλοντα fog με περιορισμένους πόρους [2]. Για fog/edge οικοσυστήματα, αντίστοιχη “πρακτική” κατεύθυνση αποτελεί και η κατανεμημένη/συνεργατική μάθηση (π.χ. federated learning), όπου τα δεδομένα παραμένουν τοπικά και ανταλλάσσονται μόνο ενημερώσεις

μοντέλων, μειώνοντας την ανάγκη μεταφοράς ακατέργαστων ευαίσθητων δεδομένων [17].

Ένα ακόμη κρίσιμο αλλά λιγότερο εξερευνημένο ζήτημα αποτελεί η εμπιστοσύνη προς τους κόμβους που συμμετέχουν στο οικοσύστημα fog. Δεδομένου ότι οι υπολογιστικοί πόροι μπορούν να προέρχονται από διαφορετικούς παρόχους ή ακόμα και από ιδιώτες, η απουσία ενός συστήματος εμπιστοσύνης καθιστά δύσκολη τη διάκριση μεταξύ αξιόπιστων και μη κόμβων. Σε περιπτώσεις όπου δεν υπάρχει μηχανισμός αξιολόγησης φήμης ή εμπιστοσύνης (trust model), τα δεδομένα ενδέχεται να αποθηκεύονται ή να υποβάλλονται σε επεξεργασία σε ανασφαλείς ή κακόβουλες συσκευές, κάτι που αντιβαίνει στις βασικές απαιτήσεις διασφάλισης της ιδιωτικότητας. Το ζήτημα αυτό εντείνεται από το γεγονός ότι στους κατανεμημένους πόρους της ομίχλης δεν υφίσταται πάντα κεντρικός έλεγχος ή πιστοποίηση. Στο edge, η ίδια ανάγκη εμφανίζεται ως lifecycle trust: ασφαλές onboarding, ανανεούμενα διαπιστευτήρια, και (όπου υποστηρίζεται) attestation/έλεγχος ακεραιότητας λογισμικού, ώστε να αποφεύγεται η συμμετοχή συμβιβασμένων κόμβων και η διάχυση παραβίασης [17]. Σε αυτό το πλαίσιο, η αξιοποίηση μηχανισμών όπως secure boot, hardware root-of-trust και remote attestation μπορεί να λειτουργήσει ως συμπληρωματική δικλείδα, επιβεβαιώνοντας ότι ένας κόμβος εκκινεί και λειτουργεί με μη αλλοιωμένο λογισμικό πριν θεωρηθεί έμπιστος.

Επιπλέον, τόσο στο fog όσο και στο edge, η φυσική έκθεση κόμβων καθιστά κρίσιμη την υιοθέτηση hardware-assisted μηχανισμών εμπιστοσύνης όπου αυτοί είναι διαθέσιμοι (secure boot, TPM-like modules, enclaves), καθώς και κρυπτογράφηση αποθηκευτικών μέσων, ώστε να μετριάζεται η εξαγωγή δεδομένων/κλειδιών σε περίπτωση κλοπής ή tampering [17].

Τέλος, εγείρεται και η ανάγκη σαφούς διαχωρισμού του fog από το edge computing στο πλαίσιο ανάλυσης των κινδύνων. Συχνά παρατηρείται σύγχυση μεταξύ των δύο εννοιών, με αποτέλεσμα να αποδίδονται στο fog χαρακτηριστικά που είναι πρακτικά εφικτά μόνο στο επίπεδο του edge. Για παράδειγμα, ορισμένες τεχνικές που βασίζονται στην επεξεργασία επί της συσκευής (on-device learning ή inference) έχουν νόημα κυρίως όταν η επεξεργασία πραγματοποιείται τοπικά, χωρίς μεταφορά των δεδομένων σε ενδιάμεσους κόμβους. Στην περίπτωση αυτή, η ιδιωτικότητα διασφαλίζεται εξ ορισμού μέσω της τοπικής επεξεργασίας, χαρακτηριστικό που παραπέμπει σε σενάρια edge computing.

Αντίθετα, στο επίπεδο του fog, όπου οι ενδιάμεσοι κόμβοι αναλαμβάνουν ρόλο συγκέντρωσης, συντονισμού ή υπολογιστική λειτουργία δεν περιορίζεται αποκλειστικά στις τερματικές συσκευές. Αυτό δεν σημαίνει ότι οι edge συσκευές παύουν να εκτελούν τοπικούς υπολογισμούς· αντίθετα, σε πολλές περιπτώσεις συνεχίζουν να πραγματοποιούν αρχική επεξεργασία ή εξαγωγή χαρακτηριστικών, ενώ οι fog κόμβοι αναλαμβάνουν πιο σύνθετες, συγκεντρωτικές ή συνεργατικές λειτουργίες. Ως εκ τούτου, σε περιβάλλοντα fog η λογική του on-device computation δεν καταργείται, αλλά εντάσσεται σε μια πολυεπίπεδη αρχιτεκτονική επεξεργασίας.

Επιπλέον, σε περιβάλλοντα που αξιοποιούν κατανεμημένη μάθηση (distributed learning) ή τεχνικές όπως το federated learning, καθίσταται εφικτή η

εκπαίδευση ή η ενημέρωση μοντέλων τόσο σε τερματικές συσκευές όσο και σε ενδιάμεσους fog κόμβους, χωρίς να απαιτείται η πλήρης αποκάλυψη των αρχικών δεδομένων σε ένα κεντρικό σημείο. Στην περίπτωση αυτή, η μάθηση δεν είναι αποκλειστικά “on-device”, αλλά λαμβάνει χώρα σε πολλαπλά επίπεδα του συστήματος, με συμμετοχή τόσο των edge/τελικών συσκευών όσο και των fog κόμβων σε μια ιεραρχική και συνεργατική διαδικασία. Η σαφής οριοθέτηση είναι κρίσιμη και για λόγους συμμόρφωσης, όπως στο πλαίσιο του GDPR, καθώς επηρεάζει τις ροές δεδομένων, τους ρόλους και τις ευθύνες των εμπλεκομένων μερών, καθώς και τις απαιτήσεις διαφάνειας και συγκατάθεσης [17].

Συνολικά, καθίσταται σαφές ότι τα προβλήματα ασφάλειας και ιδιωτικότητας στο fog computing είναι σύνθετα, πολυεπίπεδα και απαιτούν ειδική αντιμετώπιση σε κάθε στάδιο: από την αυθεντικοποίηση, την εξουσιοδότηση και την επικοινωνία, έως την αποθήκευση, την επεξεργασία και τη διαχείριση εμπιστοσύνης. Το ίδιο συμπέρασμα ισχύει και για το edge, με την πρόσθετη απαίτηση οι λύσεις να είναι ενεργειακά/υπολογιστικά αποδοτικές και να υποστηρίζουν μηχανισμούς πρόληψης–ανίχνευσης–περιορισμού–ανάκαμψης (prevention, detection, containment, recovery) σε ένα ιδιαίτερα αποκεντρωμένο πεδίο [17]. Η κατανόηση των προβλημάτων αυτών αποτελεί βασική προϋπόθεση για τον σχεδιασμό αποτελεσματικών λύσεων, ενώ η αξιοποίηση του blockchain ως συμπληρωματικού μηχανισμού ενίσχυσης ασφάλειας, εμπιστοσύνης και διαφάνειας εξετάζεται αναλυτικά στο Κεφάλαιο 5.

5. Αντιμετώπιση των Ζητημάτων στο Fog & Edge Computing με τη Χρήση του Blockchain

5.1. Ο Ρόλος του Blockchain στην Ασφάλεια του Fog & Edge Computing

Για συνοπτικότερη αποτύπωση της συμβολής του blockchain στην ασφάλεια των fog και edge περιβαλλόντων, ο παρακάτω Πίνακας 8: Συνοπτική αποτίμηση οφελών και ευκαιριών του blockchain για την ασφάλεια σε fog/edge περιβάλλοντα παρουσιάζει επιγραμματικά τα βασικά οφέλη και τις ευκαιρίες που αναδεικνύονται από την ενσωμάτωσή του στις συγκεκριμένες αρχιτεκτονικές.

Πίνακας 8: Συνοπτική αποτίμηση οφελών και ευκαιριών του blockchain για την ασφάλεια σε fog/edge περιβάλλοντα

Κατηγορία	Σημεία αποτίμησης
Οφέλη	• Ενίσχυση της ακεραιότητας και αμεταβλητότητας των καταγραφών. • Βελτίωση της ιχνηλασιμότητας και της λογοδοσίας μεταξύ πολλών κόμβων και φορέων. • Μείωση της εξάρτησης από κεντρικά σημεία εμπιστοσύνης ή ελέγχου. • Υποστήριξη αποκεντρωμένης επαλήθευσης συναλλαγών και ενεργειών. • Αυτοματοποίηση πολιτικών ασφαλείας και ελέγχου πρόσβασης μέσω smart contracts. • Ενίσχυση της λειτουργικής ανθεκτικότητας απέναντι σε σημεία αστοχίας ή επιθέσεις σε κεντρικές υποδομές.
Ευκαιρίες	• Εφαρμογή σε περιβάλλοντα πολλών οργανισμών μέσω private ή consortium blockchains. • Αξιοποίηση για ακεραιότητα και χρονική σήμανση δεδομένων αισθητήρων. • Ενσωμάτωση σε συνεργατικά οικοσυστήματα IoT, βιομηχανίας, μεταφορών και υγείας. • Συνδυασμός με μηχανισμούς attestation, trust management και anomaly detection για ισχυρότερη συνολική ασφάλεια. • Δημιουργία διαφανών audit trails για κρίσιμες ενέργειες και συμβάντα. • Υποστήριξη ασφαλέστερης διακυβέρνησης πόρων και κανόνων λειτουργίας σε κατανεμημένες υποδομές fog/edge.

Ακεραιότητα και αμεταβλητότητα καταγραφών.

Η ενσωμάτωση της τεχνολογίας blockchain στα περιβάλλοντα fog και edge computing έχει αναδειχθεί ως μία από τις πλέον ελπιδοφόρες προσεγγίσεις για

την ενίσχυση της ασφάλειας και της αξιοπιστίας αυτών των κατανεμημένων υπολογιστικών μοντέλων. Δεδομένου ότι τόσο το fog όσο και το edge computing χαρακτηρίζεται από την ύπαρξη μεγάλου αριθμού κόμβων, οι οποίοι λειτουργούν σε τοπικό επίπεδο πλησίον των τελικών συσκευών και αναλαμβάνουν την επεξεργασία και διαχείριση συχνά ευαίσθητων δεδομένων, η δημιουργία ενός ασφαλούς και ανθεκτικού συστήματος καθίσταται πρωταρχικής σημασίας.

Η υιοθέτηση του blockchain ως υποδομής ασφαλείας ανταποκρίνεται ακριβώς σε αυτή την ανάγκη, προσφέροντας ιδιότητες, όπως η ακεραιότητα των δεδομένων, η ανιχνευσιμότητα συναλλαγών και η ενίσχυση της κατανεμημένης εμπιστοσύνης. Παρότι οι αρχιτεκτονικές fog και edge στοχεύουν εγγενώς στην ανθεκτικότητα μέσω κατανομής και πλεονασμού, στην πράξη συχνά εξακολουθούν να υπάρχουν συγκεντρωτικά “σημεία εμπιστοσύνης” ή συντονισμού όπως gateways, orchestrators, control planes, κεντρικά registries ή μηχανισμοί ταυτοποίησης και πολιτικών, τα οποία μπορούν να αποτελέσουν στόχο ή σημείο αστοχίας. Σε αυτό το πλαίσιο, το blockchain μπορεί να μειώσει την εξάρτηση από κεντρικές οντότητες ως προς την καταγραφή, επικύρωση και την επιβολή κανόνων λειτουργίας, ενισχύοντας τη διαφάνεια και την ακεραιότητα της λογιστικής καταγραφής, χωρίς να προϋποθέτει έναν μοναδικό κεντρικό διαχειριστή [4],[6].

Η βασική αρχή λειτουργίας του blockchain στηρίζεται στη διατήρηση ενός κατανεμημένου μητρώου συναλλαγών, το οποίο αποθηκεύεται και ενημερώνεται ταυτόχρονα από πολλαπλούς κόμβους του δικτύου. Κάθε συναλλαγή, πριν καταχωρηθεί στο μητρώο, επικυρώνεται μέσω μηχανισμών συναίνεσης, όπως η Απόδειξη Εργασίας (Proof of Work – PoW) [1] ή η Απόδειξη Συμμετοχής (Proof of Stake – PoS), εξασφαλίζοντας ότι το περιεχόμενο της συναλλαγής είναι έγκυρο και αμετάβλητο. Αυτό το χαρακτηριστικό της αναλλοίωτης καταγραφής (immutability) διαδραματίζει καθοριστικό ρόλο στην προστασία των fog/edge περιβαλλόντων, διότι διασφαλίζει ότι οποιαδήποτε δραστηριότητα στους κόμβους του fog περιβάλλοντος παραμένει καταγεγραμμένη και μη επιδεχόμενη αλλοιώσεις εκ των υστέρων [4].

Αποκεντρωμένη εμπιστοσύνη και όρια του blockchain.

Υπό το πρίσμα αυτό, το blockchain μπορεί να συμβάλει ουσιαστικά στην αποκεντρωμένη διαχείριση της εμπιστοσύνης μεταξύ των διάσπαρτων κόμβων του fog. Σε περιβάλλοντα fog και edge, όπου οι κόμβοι ανήκουν συχνά σε διαφορετικούς φορείς και λειτουργούν υπό ετερογενή θεσμικά και τεχνολογικά πλαίσια, η απουσία μίας ενιαίας κεντρικής αρχής πιστοποίησης μπορεί να ευνοήσει φαινόμενα κατάχρησης, παραποίησης ή αμφισβήτησης της αξιοπιστίας των δεδομένων. Στο πλαίσιο αυτό, το blockchain λειτουργεί ως μηχανισμός αποκεντρωμένης επαλήθευσης και καταγραφής, επιτρέποντας στους κόμβους να επιβεβαιώνουν τη γνησιότητα συναλλαγών και ενεργειών χωρίς την παρέμβαση τρίτου μεσολαβητή [6]. Ωστόσο, η συμβολή του δεν είναι απόλυτη ούτε επαρκεί από μόνη της για την πλήρη θεμελίωση ενός μοντέλου εμπιστοσύνης. Ειδικότερα, στην περίπτωση όπου ένας κόμβος είναι εξ αρχής κακόβουλος ή έχει περιέλθει υπό τον έλεγχο επιτιθέμενου, το blockchain δεν μπορεί να διασφαλίσει ότι τα δεδομένα που εισάγει ή οι ενέργειες που εκτελεί

είναι κατ' ουσίαν αξιόπιστα. Κατά συνέπεια, το blockchain δεν υποκαθιστά το trust model, αλλά αποτελεί επιμέρους δομικό στοιχείο του, το οποίο πρέπει να συνδυάζεται με συμπληρωματικούς μηχανισμούς, όπως ισχυρή αυθεντικοποίηση, έλεγχο πρόσβασης, απομακρυσμένη πιστοποίηση ακεραιότητας (remote attestation), μηχανισμούς ανίχνευσης ανωμαλιών και πολιτικές διαχείρισης εμπιστοσύνης. Υπό αυτήν την έννοια, το blockchain ενισχύει ιδιότητες όπως η ακεραιότητα, η ιχνηλασιμότητα και η λογοδοσία, περιορίζοντας ορισμένες κατηγορίες επιθέσεων που σχετίζονται με την ύπαρξη κεντρικών σημείων ελέγχου ή με την παραπλάνηση κόμβων, χωρίς όμως να εξαλείφει συνολικά τον κίνδυνο από παραβιασμένους ή κακόβουλους κόμβους.

Αυθεντικότητα επικοινωνιών και ψηφιακές υπογραφές.

Ιδιαίτερη σημασία έχει η διασφάλιση της αυθεντικότητας των επικοινωνιών μεταξύ των κόμβων. Μέσω της χρήσης κρυπτογραφικών μηχανισμών και ψηφιακών υπογραφών, που συνοδεύουν κάθε συναλλαγή εντός του blockchain, καθίσταται εφικτή η επαλήθευση της ταυτότητας των εμπλεκομένων μερών και η αποτροπή εισαγωγής ψευδών δεδομένων από κακόβουλους φορείς [4]. Η δυνατότητα αυτή είναι ιδιαιτέρως κρίσιμη στο edge computing, όπου πολλά τερματικά σημεία είναι συσκευές IoT με περιορισμένες εγγενείς δυνατότητες ασφαλείας και αυξημένη έκθεση σε υποκλοπές ή παραβιάσεις [5].

Λειτουργική ανθεκτικότητα και ανθεκτικότητα υπηρεσιών.

Εξίσου σημαντική είναι η συμβολή του blockchain στη λειτουργική ανθεκτικότητα (operational resilience) των δεδομένων και των υπηρεσιών. Αν και τα fog και edge περιβάλλοντα είναι ήδη κατανεμημένα, στην πράξη μπορεί να υφίστανται «πηγές αλήθειας» ή μηχανισμοί συντονισμού που αποτελούν ελκυστικούς στόχους DDoS ή σημεία αστοχίας. Η αποκεντρωμένη καταγραφή και επικύρωση που παρέχει το blockchain μπορεί να περιορίσει την εξάρτηση από τέτοια σημεία και να συμβάλει στη συνέχιση κρίσιμων λειτουργιών ακόμη και όταν μέρος των κόμβων τεθεί εκτός λειτουργίας [6]. Σε αντίθεση με παραδοσιακές κεντρικές αρχιτεκτονικές, όπου η κατάρρευση του κεντρικού εξυπηρετητή μπορεί να οδηγήσει σε συνολική διακοπή υπηρεσιών, στα αποκεντρωμένα δίκτυα η λειτουργία του συστήματος μπορεί να συνεχιστεί με μεγαλύτερη ανθεκτικότητα.

Τύποι blockchain και καταλληλότητα για fog/edge περιβάλλοντα.

Ειδικότερα, αξίζει να υπογραμμιστεί ότι στο πλαίσιο του fog και edge computing, το blockchain μπορεί να εφαρμοστεί με διαφορετικά μοντέλα συμμετοχής και ελέγχου πρόσβασης (public, private, consortium), τα οποία επηρεάζουν έμμεσα ζητήματα διακυβέρνησης και—δευτερευόντως—ιδιωτικότητας. Οι δημόσιες αλυσίδες (public blockchains), όπως το Bitcoin, επιτρέπουν σε οποιονδήποτε να συμμετέχει ελεύθερα στη διαδικασία επικύρωσης των συναλλαγών, όμως συχνά συνοδεύονται από αυξημένες απαιτήσεις υπολογιστικής ισχύος και καθυστερήσεις συναλλαγών, γεγονός που μπορεί να επηρεάσει αρνητικά εφαρμογές edge computing με απαιτήσεις πραγματικού χρόνου [8]. Αντίθετα, οι ιδιωτικές αλυσίδες (private blockchains) προσφέρουν περιορισμένη πρόσβαση μόνο σε εξουσιοδοτημένους κόμβους,

εξασφαλίζοντας μεγαλύτερο έλεγχο και καλύτερη απόδοση [8], [9]. Οι κοινοπρακτικές αλυσίδες (consortium blockchains) αποτελούν ενδιάμεση λύση, κατά την οποία η διαδικασία συναίνεσης επιτελείται από προκαθορισμένο σύνολο εμπιστευμένων οντοτήτων, γεγονός που τις καθιστά ιδιαίτερα κατάλληλες για εφαρμογή σε συνεργατικά fog/edge περιβάλλοντα πολλών οργανισμών [10]. Παρότι το μοντέλο πρόσβασης επηρεάζει το επίπεδο έκθεσης πληροφοριών, η ιδιωτικότητα στο blockchain δεν εξαντλείται σε αυτό· εξαρτάται επίσης από το τι γράφεται on-chain, τι μένει off-chain, πώς γίνεται η κρυπτογράφηση/διαχείριση κλειδιών και ποιοι μηχανισμοί επιτρέπουν έλεγχο χωρίς αποκάλυψη. Τα ζητήματα αυτά αναλύονται στην επόμενη ενότητα.

Έξυπνα συμβόλαια και αυτοματοποίηση πολιτικών ασφαλείας.

Ακόμα περισσότερο, σημαντικό ρόλο στην προστασία του fog και edge computing διαδραματίζει η ενσωμάτωση έξυπνων συμβολαίων (smart contracts), δηλαδή αυτοεκτελούμενων προγραμμάτων που ενεργοποιούνται αυτόματα όταν πληρούνται συγκεκριμένες προϋποθέσεις. Τα έξυπνα συμβόλαια επιτρέπουν την αυτοματοποίηση κρίσιμων λειτουργιών, όπως ο έλεγχος πρόσβασης, η καταγραφή αλληλεπιδράσεων ή η διαχείριση των πόρων των κόμβων, εξαλείφοντας ταυτόχρονα τον ανθρώπινο παράγοντα που συχνά αποτελεί ευάλωτο σημείο ως προς την ασφάλεια [4]. Για παράδειγμα, σε περίπτωση που ένας κόμβος fog ή edge επιχειρήσει να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε δεδομένα, ένα έξυπνο συμβόλαιο μπορεί να διακόψει αυτόματα την επικοινωνία και να ενημερώσει το υπόλοιπο δίκτυο. Επιπλέον, τα έξυπνα συμβόλαια δεν περιορίζονται μόνο σε μεμονωμένους ελέγχους πρόσβασης, αλλά μπορούν να αποτυπώσουν και να αυτοματοποιήσουν βασικές διαδικασίες λειτουργίας ενός συστήματος, όπως την εγγραφή/απενεργοποίηση κόμβων, την επιβολή πολιτικών χρήσης πόρων (quotas), τη διαχείριση κανόνων συνεργασίας μεταξύ φορέων και τη δημιουργία αμετάβλητων audit trails για κρίσιμες ενέργειες. Ωστόσο, η χρήση τους είναι καταλληλότερη για ντετερμινιστικούς κανόνες διακυβέρνησης και ελέγχου, ενώ λειτουργίες με αυστηρές απαιτήσεις πραγματικού χρόνου ή υψηλό υπολογιστικό φορτίο τυπικά παραμένουν εκτός αλυσίδας (off-chain), καθώς η on-chain εκτέλεση μπορεί να επιβαρύνει την απόδοση και την καθυστέρηση [4]. Το σημείο αυτό είναι ιδιαίτερα κρίσιμο σε εφαρμογές όπως η βιομηχανική αυτοματοποίηση ή η αυτόνομη οδήγηση, όπου ακόμη και μικρές καθυστερήσεις είναι δυνατόν να έχουν σοβαρές επιπτώσεις.

Ακεραιότητα και χρονική σήμανση δεδομένων αισθητήρων

Αναλύοντας ακόμα περισσότερο, το blockchain συμβάλλει στη διασφάλιση της ακεραιότητας των δεδομένων αισθητήρων που συλλέγονται και επεξεργάζονται σε περιβάλλοντα fog και edge. Δεδομένου ότι οι αισθητήρες λειτουργούν ως αρχικοί πάροχοι πληροφορίας, τυχόν αλλοίωση των δεδομένων τους μπορεί να οδηγήσει σε παραπλανητικές αποφάσεις ή σε διατάραξη κρίσιμων διαδικασιών. Η καταγραφή των δεδομένων αισθητήρων σε blockchain καθιστά δυνατή την εξακρίβωση της αυθεντικότητας και της ακριβούς χρονικής στιγμής συλλογής τους, ενισχύοντας έτσι την αξιοπιστία της συνολικής αρχιτεκτονικής [5].

Τομείς εφαρμογής και πρακτική αξιοποίηση.

Εξετάζοντας τις πρακτικές εφαρμογές της σύζευξης fog/edge computing και blockchain, διαπιστώνεται ότι οι περισσότερες προσεγγίσεις βρίσκονται ακόμη σε ερευνητικό ή πρωτοτυπικό στάδιο. Παρ' όλα αυτά, η βιβλιογραφία αναδεικνύει κρίσιμους τομείς ως ιδιαίτερα πρόσφορους για την αξιοποίηση του blockchain σε κατανεμημένα περιβάλλοντα κοντά στην άκρη του δικτύου—όπως οι αλυσίδες εφοδιασμού, οι χρηματοοικονομικές υπηρεσίες, οι βιομηχανικές εφαρμογές, οι μεταφορές και εφαρμογές υγείας—όπου απαιτούνται ακεραιότητα, ιχνηλασιμότητα, αυθεντικότητα και διαφανής διαμοιρασμός δεδομένων μεταξύ πολλών φορέων [2], [4], [5], [11], [12] .

Συνολική αποτίμηση.

Συνοψίζοντας τις παραπάνω παρατηρήσεις, καθίσταται σαφές ότι το blockchain αποτελεί μια καινοτόμο προσέγγιση για την αντιμετώπιση των σύνθετων ζητημάτων ασφάλειας στο fog και edge computing. Η αρχή της κατανεμημένης εμπιστοσύνης, η αμετάβλητη καταγραφή δεδομένων, η διασφάλιση της ακεραιότητας και της αυθεντικότητας, η ενίσχυση της λειτουργικής ανθεκτικότητας και η αυτοματοποίηση διαδικασιών μέσω έξυπνων συμβολαίων προσφέρουν ένα πλαίσιο προστασίας που συνάδει με τη φύση των κατανεμημένων υπολογιστικών συστημάτων. Εφάμιλλα, οι διαφορετικοί τύποι αλυσίδων επιτρέπουν την προσαρμογή της λύσης στις εκάστοτε λειτουργικές και οργανωτικές απαιτήσεις, καθιστώντας το blockchain ένα πολυδιάστατο εργαλείο στην κατεύθυνση της ενίσχυσης της ασφάλειας και της αξιοπιστίας των fog και edge αρχιτεκτονικών [4], [8], [10].

5.2. Ο Ρόλος του Blockchain στη Διατήρηση της Ιδιωτικότητας του Fog & Edge Computing

Αντίστοιχα, για τη συστηματικότερη αποτίμηση της συμβολής του blockchain στη διατήρηση της ιδιωτικότητας σε fog και edge περιβάλλοντα, ο Πίνακας 9:

Συνοπτική αποτίμηση οφελών και ευκαιριών του blockchain για την ιδιωτικότητα σε fog/edge περιβάλλοντα συνοψίζει τα βασικά οφέλη και τις ευκαιρίες που προκύπτουν από την ενσωμάτωσή του.

Πίνακας 9: Συνοπτική αποτίμηση οφελών και ευκαιριών του blockchain για την ιδιωτικότητα σε fog/edge περιβάλλοντα

Κατηγορία	Σημεία αποτίμησης
Δυνάμεις (Strengths)	• Αποκεντρωμένη διακυβέρνηση και μείωση σημείων μοναδικής εμπιστοσύνης. • Ακεραιότητα και αμεταβλητότητα καταγραφών, που ενισχύουν την ιχνηλασιμότητα και τη λογοδοσία. • Δυνατότητα επιβολής δυναμικών πολιτικών ελέγχου πρόσβασης μέσω smart contracts. • Υποστήριξη ελεγχόμενης διαμοίρασης δεδομένων σε περιβάλλοντα πολλών φορέων. • Ενίσχυση της διαφάνειας ως προς το ποιος απέκτησε πρόσβαση, πότε και υπό ποιες προϋποθέσεις. • Δυνατότητα συνδυασμού με off-chain αποθήκευση, ώστε να περιορίζεται η άμεση έκθεση ευαίσθητων δεδομένων on-chain. • Υποστήριξη μοντέλων ελαχιστοποίησης ανταλλαγής δεδομένων και τοπικής επεξεργασίας.
Αδυναμίες (Weaknesses)	• Η αμεταβλητότητα της αλυσίδας μπορεί να συγκρούεται με απαιτήσεις διαγραφής ή διόρθωσης δεδομένων, όπως το δικαίωμα στη λήθη. • Η ψευδωνυμοποίηση και το hashing δεν επαρκούν από μόνα τους για πλήρη προστασία της ιδιωτικότητας. • Παραμένει ο κίνδυνος συσχέτισης συναλλαγών και επαναταυτοποίησης μέσω quasi-identifiers και metadata. • Αυξημένο υπολογιστικό και επικοινωνιακό κόστος, ιδίως σε edge συσκευές με περιορισμένους πόρους. • Εξάρτηση από ορθή διαχείριση κλειδιών, πιστοποιητικών και μηχανισμών ταυτότητας. • Το blockchain δεν μπορεί να εγγυηθεί την αξιοπιστία των δεδομένων που εισάγονται από κακόβουλους ή παραβιασμένους κόμβους. • Πιθανές ευπάθειες σε smart contracts ή σε λανθασμένη υλοποίηση πολιτικών πρόσβασης. • Υψηλό υπολογιστικό και λειτουργικό κόστος κατά τον συνδυασμό blockchain με προηγμένες κρυπτογραφικές τεχνικές, όπως ZKPs και ομομορφική κρυπτογράφηση.
Ευκαιρίες (Opportunities)	• Συνδυασμός με federated learning για περιορισμό της μεταφοράς ακατέργαστων προσωπικών δεδομένων. • Αξιοποίηση προηγμένων τεχνικών, όπως zero-knowledge proofs και homomorphic encryption, για ενισχυμένη προστασία ιδιωτικότητας. • Ανάπτυξη user-centric ή patient-centric μοντέλων ελέγχου πρόσβασης και διαχείρισης συγκατάθεσης.

Κατηγορία	Σημεία αποτίμησης
	• Εφαρμογή σε τομείς υψηλής ευαισθησίας, όπως υγεία, βιομηχανικό IoT και φαρμακευτική εφοδιαστική αλυσίδα. • Δημιουργία πλαισίων διακυβέρνησης σε consortium blockchains μεταξύ συνεργαζόμενων οργανισμών. • Ενίσχυση της κανονιστικής συμμόρφωσης μέσω επαληθεύσιμης καταγραφής ενεργειών και προσβάσεων.
Απειλές (Threats)	• Παραβιασμένοι ή κακόβουλοι fog/edge κόμβοι μπορούν να εισάγουν ψευδή, παραποιημένα ή ευαίσθητα δεδομένα στην αλυσίδα ή στο συνοδό σύστημα. • Επιθέσεις συσχέτισης, ανάλυσης μεταδεδομένων και linkability μπορούν να οδηγήσουν σε αποκάλυψη ταυτότητας, τοποθεσίας ή προτύπων χρήσης. • Διαρροή ή κλοπή ιδιωτικών κλειδιών μπορεί να επιτρέψει μη εξουσιοδοτημένη πρόσβαση ή κατάχρηση ταυτότητας. • Επιθέσεις σε έξυπνα συμβόλαια, σε permissioned μηχανισμούς ή σε off-chain αποθηκευτικούς χώρους μπορούν να ακυρώσουν μέρος της προστασίας. • Συμπαιγνία μεταξύ συμμετεχόντων ή προβλήματα διακυβέρνησης σε consortium περιβάλλοντα μπορούν να υπονομεύσουν την εμπιστοσύνη. • Νομικές και κανονιστικές αβεβαιότητες σχετικά με δικαιοδοσία, διαγραφή δεδομένων, λογοδοσία και συμμόρφωση με τον GDPR. • Η υπερβολική εμπιστοσύνη στο blockchain ως «ολική λύση» μπορεί να οδηγήσει σε υποεκτίμηση άλλων αναγκαίων μηχανισμών ασφαλείας και ιδιωτικότητας.
	•

Ιδιωτικότητα ως αποκεντρωμένη διακυβέρνηση και έλεγχος.

Η διασφάλιση της ιδιωτικότητας σε περιβάλλοντα fog και edge computing αποτελεί μια πρόκληση αυξανόμενης σημασίας, καθώς η αποκεντρωμένη φύση αυτής της αρχιτεκτονικής καθιστά τη διαχείριση και την προστασία των προσωπικών δεδομένων περίπλοκη. Τεράστιος όγκος προσωπικών και ευαίσθητων πληροφοριών παράγεται, επεξεργάζεται και διακινείται κοντά στις πηγές δεδομένων και συχνά σε πραγματικό χρόνο, γεγονός που πολλαπλασιάζει τις πιθανότητες παραβίασης ιδιωτικότητας. Η αξιοποίηση της τεχνολογίας blockchain, πέραν της ενίσχυσης της ασφάλειας, έχει αναγνωριστεί ως μια προοδευτική λύση και στον τομέα της προστασίας της ιδιωτικότητας, διαμορφώνοντας νέες προσεγγίσεις ως προς τον τρόπο με τον οποίο αποθηκεύονται, διακινούνται και ελέγχονται τα δεδομένα [4].

Η ιδιωτικότητα, ως έννοια, στο πλαίσιο του fog και edge computing, δεν περιορίζεται αποκλειστικά στην απόκρυψη προσωπικών πληροφοριών, αλλά

εκτείνεται στη δυνατότητα των χρηστών να έχουν τον πλήρη έλεγχο της διαχείρισης των δεδομένων τους, αποφασίζοντας ποιος, πότε και υπό ποιες προϋποθέσεις θα έχει πρόσβαση σε αυτά. Η ανάγκη για αυστηρότερη προστασία καθίσταται επιτακτική λόγω της κατανομής των υπολογιστικών διεργασιών σε πολλαπλούς κόμβους, οι οποίοι συχνά λειτουργούν σε διαφορετικά επίπεδα εμπιστοσύνης και ανήκουν σε ετερογενείς φορείς. Σε αυτό το πλαίσιο, το blockchain εισάγει μηχανισμούς που επιτρέπουν την προστασία των προσωπικών δεδομένων, διατηρώντας παράλληλα τη λειτουργικότητα και την αποδοτικότητα των εφαρμογών [5].

Ακεραιότητα, auditability και έλεγχος ροής δεδομένων.

Κεντρικός πυλώνας της συνεισφοράς του blockchain στη θωράκιση της ιδιωτικότητας στα συστήματα fog/edge δεν είναι η «αποκέντρωση» καθαυτή, αφού οι αρχιτεκτονικές αυτές είναι ήδη κατανεμημένες, αλλά η αποκεντρωμένη διακυβέρνηση και η μείωση των σημείων μοναδικής εμπιστοσύνης (single points of trust) κατά τη διαχείριση και την καταγραφή κρίσιμων ενεργειών [4]. Παρότι τα προσωπικά δεδομένα συχνά συλλέγονται και επεξεργάζονται κοντά στην πηγή, στην πράξη ενδέχεται να συγκεντρώνονται σε ενδιάμεσους κόμβους, όπως gateways ή aggregators, να συγχρονίζονται ή να αποστέλλονται προς το νέφος για αποθήκευση και περαιτέρω ανάλυση. Επομένως, το blockchain μπορεί να συμβάλει κυρίως ως μηχανισμός ακεραιότητας και ιχνηλασιμότητας (auditability), καταγράφοντας ποιος, πότε και υπό ποιες πολιτικές απέκτησε πρόσβαση ή προώθησε δεδομένα, καθώς και ως μέσο επιβολής πολιτικών πρόσβασης σε περιβάλλοντα πολλών φορέων, περιορίζοντας την εξάρτηση από έναν κεντρικό διαχειριστή [4].

Επιπλέον, παρότι το νέφος διαθέτει συχνά ισχυρότερη φυσική θωράκιση και ώριμες διαδικασίες ασφάλειας, η διασπορά των δεδομένων μεταξύ edge, fog και cloud, καθώς και η εμπλοκή πολλών οντοτήτων, εξακολουθούν να δημιουργούν κινδύνους ιδιωτικότητας, όπως μη διαφανείς ροές δεδομένων, συσχετισμούς και υπερσυγκέντρωση πληροφορίας. Το blockchain δεν αναιρεί από μόνο του αυτούς τους κινδύνους, αλλά μπορεί να τους μετριάσει μέσω διαφάνειας, ελέγχου, λογοδοσίας και ακεραιότητας στη ροή επεξεργασίας.

Ψευδωνυμοποίηση και hashing

Ένας από τους βασικότερους τρόπους με τους οποίους το blockchain συμβάλλει στη διατήρηση της ιδιωτικότητας είναι η χρήση κρυπτογραφικών τεχνικών, όπως η ψευδωνυμοποίηση και η κατακερματισμένη αποθήκευση. Αντί της απευθείας καταγραφής προσωπικών δεδομένων στο κατανεμημένο μητρώο, οι πληροφορίες αυτές αντικαθίστανται από μοναδικά αναγνωριστικά (hash values), τα οποία δεν αποκαλύπτουν ευθέως τα πραγματικά στοιχεία των χρηστών. Με αυτόν τον τρόπο, ακόμη και αν κακόβουλοι παράγοντες αποκτήσουν πρόσβαση στο blockchain, δεν θα είναι άμεσα σε θέση να ταυτοποιήσουν συγκεκριμένα άτομα [4].

Ψευδωνυμοποίηση/Hashing

Η ψευδωνυμοποίηση και η κατακερματισμένη αποθήκευση (hashing) δεν ισοδυναμούν με “πλήρη” προστασία ευαίσθητων δεδομένων. Ο

κατακερματισμός είναι κατά κανόνα μη αναστρέψιμος, όμως δεν αποτρέπει την αποκάλυψη όταν τα αρχικά δεδομένα προέρχονται από μικρό ή προβλέψιμο χώρο τιμών (π.χ. ημερομηνίες, ταχυδρομικοί κώδικες, περιορισμένες κατηγορίες), καθώς ο επιτιθέμενος μπορεί να εφαρμόσει dictionary/rainbow-table επιθέσεις και να αντιστοιχίσει hash → τιμή. Για τον λόγο αυτό, όταν γίνεται hashing ευαίσθητων πεδίων, απαιτούνται πρακτικές όπως salt (και όπου ενδείκνυται pepper/HMAC), ώστε να μειώνεται η δυνατότητα προϋπολογισμένων αντιστοιχίσεων. Επιπλέον, η "κατακερματισμένη αποθήκευση" χρησιμοποιείται συχνά ως μηχανισμός ακεραιότητας (δηλ. δέσμευση/δέσιμο προς off-chain δεδομένα) και όχι ως αυτάρκης τεχνική εμπιστευτικότητας.

Οιωνεί αναγνωριστικά και κίνδυνος επαναταυτοποίησης.

Οιωνεί αναγνωριστικά (quasi-identifiers).

Τα οιωνεί χαρακτηριστικά δεν προστατεύονται με τον ίδιο τρόπο απλώς και μόνο επειδή "δεν γράφονται ονοματεπώνυμα". Ακόμη και αν αποθηκεύονται ως hashes, η συσχέτιση πολλαπλών πεδίων (π.χ. ηλικία–περιοχή–χρόνος) ή η ύπαρξη εξωτερικών πηγών (auxiliary datasets) μπορεί να οδηγήσει σε re-identification. Σε blockchain περιβάλλοντα, ο κίνδυνος αυτός αυξάνεται επειδή οι συναλλαγές είναι συχνά διαχρονικά συσχετίσιμες (linkability): το ίδιο ψευδώνυμο/διεύθυνση μπορεί να επανεμφανίζεται και να αποκαλύπτει πρότυπα χρήσης ή συμπεριφοράς. Συνεπώς, η προστασία quasi-identifiers απαιτεί συνδυασμό τεχνικών: ελαχιστοποίηση των μεταδεδομένων που γράφονται on-chain, αποφυγή αποθήκευσης ευαίσθητων/quasi πεδίων ακόμη και ως hash, και χρήση πρόσθετων μηχανισμών όπως off-chain αποθήκευση και επιλεκτική αποκάλυψη (selective disclosure) όπου χρειάζεται.

Ταυτοποίηση κόμβων/χρηστών και linkability.

Ταυτοποίηση κόμβων/χρηστών

Η δυνατότητα ταυτοποίησης ενός ατόμου από το blockchain εξαρτάται από το μοντέλο συμμετοχής και ταυτότητας. Σε public blockchains, οι διευθύνσεις είναι ψευδώνυμες, αλλά μπορούν να ταυτοποιηθούν αν συσχετιστούν με εξωτερικά δεδομένα (π.χ. logs, υπηρεσίες, σημεία εισόδου/εξόδου) ή αν το ίδιο ψευδώνυμο χρησιμοποιείται επανειλημμένα. Σε private/consortium blockchains, όπου η συμμετοχή είναι permissioned, συχνά υπάρχουν ψηφιακά πιστοποιητικά (PKI) ή μηχανισμοί εγγραφής με πραγματική ταυτότητα· σε αυτή την περίπτωση, η ταυτοποίηση είναι τεχνικά εφικτή από τους εξουσιοδοτημένους φορείς (π.χ. CA/διαχειριστής κοινοπραξίας), και το ζητούμενο μετατοπίζεται από την "ανωνυμία" στην ελεγχόμενη αποκάλυψη και στη διακυβέρνηση πρόσβασης.

Για τον περιορισμό του κινδύνου, εφαρμόζονται πρακτικές όπως: (α) περιοδική αλλαγή ψευδωνύμων/διευθύνσεων ώστε να μειώνεται η συνδεσιμότητα (linkability), (β) αποθήκευση ευαίσθητων δεδομένων εκτός αλυσίδας (off-chain) και καταγραφή on-chain μόνο δεικτών/δεσμεύσεων (hash pointers) για σκοπούς ακεραιότητας, (γ) αυστηρός έλεγχος πρόσβασης σε permissioned δίκτυα (ποιος βλέπει τι), και (δ) αποφυγή καταγραφής μεταδεδομένων που

μπορούν να λειτουργήσουν ως quasi-identifiers. Έτσι, το blockchain μπορεί να ενισχύσει τη διαφάνεια και την ακεραιότητα χωρίς να μετατραπεί σε μόνιμο αποθετήριο προσωπικών πληροφοριών [4].

Off-chain αποθήκευση και πρόσθετες τεχνικές προστασίας.

Πέραν των ανωτέρω, η ενίσχυση της ιδιωτικότητας σε blockchain περιβάλλοντα απαιτεί συχνά πρόσθετες κρυπτογραφικές και αρχιτεκτονικές τεχνικές προστασίας. Οι τεχνικές αυτές αφορούν κυρίως (i) το περιεχόμενο των συναλλαγών/δεδομένων (payload), ώστε να μην είναι αναγνώσιμο από μη εξουσιοδοτημένους συμμετέχοντες, και (ii) τα μεταδεδομένα και τη συσχετιστική πληροφορία, όπως η συνδεσιμότητα διευθύνσεων (linkability), οι χρονισμοί και τα πρότυπα συναλλαγών, που μπορούν να οδηγήσουν σε έμμεση ταυτοποίηση. Στην πράξη, αυτό επιτυγχάνεται με κρυπτογράφηση ή/και αποθήκευση των ευαίσθητων δεδομένων εκτός αλυσίδας (off-chain) και καταγραφή on-chain μόνο δεικτών ακεραιότητας (hash pointers), καθώς και με μηχανισμούς όπως η ψευδωνυμοποίηση, η συχνή αλλαγή διευθύνσεων και, όπου απαιτείται ισχυρότερη προστασία, τεχνικές επιλεκτικής αποκάλυψης ή αποδείξεις μηδενικής γνώσης [9].

Data minimization και τοπική διατήρηση δεδομένων.

Σε προέκταση των προηγουμένων, ιδιαίτερη σημασία αποκτά η εφαρμογή μοντέλων ελαχιστοποίησης της ανταλλαγής δεδομένων (data minimization). Στο πλαίσιο αυτό, το blockchain επιτρέπει τη δημιουργία αρχιτεκτονικών όπου μόνο τα απολύτως απαραίτητα δεδομένα διαμοιράζονται μεταξύ των κόμβων του fog και edge computing, ενώ οι υπόλοιπες ευαίσθητες πληροφορίες παραμένουν τοπικά αποθηκευμένες στις συσκευές των χρηστών ή σε προστατευμένους κόμβους. Η πρακτική αυτή καθίσταται ιδιαίτερα χρήσιμη σε τομείς όπως η υγειονομική περίθαλψη, όπου η διατήρηση του ιατρικού απορρήτου είναι ζωτικής σημασίας. Πράγματι, μελέτες έχουν αναδείξει τη χρησιμότητα του blockchain στη διαχείριση ιατρικών δεδομένων, καθώς διασφαλίζει ότι μόνο εξουσιοδοτημένοι φορείς μπορούν να αποκτήσουν πρόσβαση σε κρίσιμες πληροφορίες, διατηρώντας ταυτόχρονα την ακεραιότητα των αρχείων υγείας [7].

Έλεγχος πρόσβασης μέσω smart contracts.

Ένας ακόμα παράγοντας που καθιστά το blockchain πολύτιμο εργαλείο στη διατήρηση της ιδιωτικότητας στο fog computing αφορά τις δυνατότητες ελέγχου πρόσβασης (access control). Όπως ήδη αναφέρθηκε στην Ενότητα 6.1, τα έξυπνα συμβόλαια (smart contracts) μπορούν να αξιοποιηθούν ως μηχανισμοί αυτοματοποιημένης επιβολής κανόνων και πολιτικών μέσα σε ένα blockchain περιβάλλον. Στο πλαίσιο της ιδιωτικότητας, η λειτουργία αυτή αποκτά ιδιαίτερη σημασία, καθώς μέσω της χρήσης έξυπνων συμβολαίων, δύναται να εφαρμοστούν δυναμικές πολιτικές ελέγχου, οι οποίες καθορίζουν με σαφήνεια τα επίπεδα πρόσβασης και τους όρους υπό τους οποίους οι κόμβοι ή οι τελικοί χρήστες θα μπορούν να επεξεργαστούν συγκεκριμένα δεδομένα. Αυτές οι διαδικασίες αυτοματοποιούνται και καταγράφονται στο blockchain, με αποτέλεσμα να αποτρέπονται αυθαίρετες ενέργειες από μη εξουσιοδοτημένους φορείς και να ενισχύονται η ιχνηλασιμότητα και η λογοδοσία [5]. Ειδικά σε

private ή consortium blockchains, οι οργανισμοί μπορούν να καθορίζουν με μεγαλύτερη ακρίβεια ποιοι κόμβοι και ποιες οντότητες διαθέτουν δικαίωμα ανάγνωσης, τροποποίησης ή επικύρωσης δεδομένων [9].

Διαχείριση δικαιωμάτων χρηστών και συγκατάθεσης.

Σημαντική είναι, επίσης, η συμβολή του blockchain στη διαχείριση των δικαιωμάτων των χρηστών (user rights management). Οι χρήστες δύνανται να ορίζουν, μέσω αποκεντρωμένων μηχανισμών, τις παραμέτρους κάτω από τις οποίες τα δεδομένα τους θα διαμοιράζονται. Αυτή η προσέγγιση αποκτά ιδιαίτερη αξία σε περιβάλλοντα όπου η τήρηση κανονιστικών πλαισίων, όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR), καθίσταται απαραίτητη. Στο πλαίσιο αυτό, έχει προταθεί η εφαρμογή blockchain συστημάτων που επιτρέπουν την καταγραφή της συγκατάθεσης των χρηστών με τρόπο που διασφαλίζει ότι οι όροι που αυτοί θέτουν δεν μπορούν να παρακαμφθούν εκ των υστέρων [11].

Τύποι blockchain και επιπτώσεις στην ιδιωτικότητα.

Αξιοσημείωτη είναι και η διαφοροποίηση των τύπων blockchain ως προς την προστασία της ιδιωτικότητας. Τα ιδιωτικά blockchains (private blockchains) παρέχουν αυξημένο έλεγχο πρόσβασης και μεγαλύτερη δυνατότητα περιορισμού της ορατότητας των δεδομένων, επιτρέποντας τη συμμετοχή μόνο σε συγκεκριμένα, έμπιστα μέλη. Για τον λόγο αυτό, θεωρούνται ιδιαίτερα κατάλληλα για περιβάλλοντα fog και edge, όπου απαιτείται υψηλή διαβάθμιση εμπιστευτικότητας και σαφέστερη διακυβέρνηση πρόσβασης. Αντίθετα, τα δημόσια blockchains (public blockchains), αν και προσφέρουν υψηλό βαθμό διαφάνειας και επαληθευσιμότητας, εγείρουν εντονότερες ανησυχίες ως προς την ιδιωτικότητα, λόγω της ευρύτερης έκθεσης μεταδεδομένων και της δυνατότητας συσχέτισης συναλλαγών ή διευθύνσεων [9]. Οι κοινοπρακτικές αλυσίδες (consortium blockchains) τοποθετούνται μεταξύ των δύο αυτών προσεγγίσεων, συνδυάζοντας στοιχεία ελεγχόμενης συμμετοχής και κατανεμημένης διακυβέρνησης, γεγονός που τις καθιστά ιδιαίτερα κατάλληλες για fog περιβάλλοντα όπου συνεργάζονται πολλαπλοί οργανισμοί με κοινά επιχειρησιακά ή θεσμικά συμφέροντα [5].

Blockchain και federated learning.

Εντός του ιδίου πλαισίου, αξίζει να σημειωθεί ότι το blockchain μπορεί να συνδυαστεί με τεχνολογίες ομοσπονδιακής μάθησης (federated learning), επιτρέποντας την επεξεργασία δεδομένων σε τοπικό επίπεδο χωρίς την ανάγκη μεταφοράς τους σε κεντρικό αποθηκευτικό χώρο. Πιο συγκεκριμένα, ο ρόλος του blockchain στη σύζευξη με ομοσπονδιακή μάθηση δεν είναι η άμεση επεξεργασία ή αποθήκευση των προσωπικών δεδομένων, αλλά η επιβολή των όρων συμμετοχής και πρόσβασης στο σχήμα μάθησης: μέσω ενός permissioned μηχανισμού ή/και smart contracts μπορεί να καθορίζεται ποιοι κόμβοι έχουν δικαίωμα να συμμετέχουν, υπό ποιες πολιτικές (π.χ. ρόλοι, τοποθεσία, επίπεδο εμπιστοσύνης), καθώς και να καταγράφεται αμετάβλητα η ανταλλαγή ενημερώσεων μοντέλου (model updates) για λόγους ιχνηλασιμότητας και λογοδοσίας [5]. Η σύζευξη αυτών των τεχνολογιών ενδυναμώνει τις δυνατότητες προστασίας της ιδιωτικότητας, καθώς τα

δεδομένα παραμένουν τοπικά και το blockchain περιορίζει/ελέγχει ποιοι κόμβοι μπορούν να συμμετέχουν και να λαμβάνουν ή να αποστέλλουν ενημερώσεις, μειώνοντας την έκθεση σε μη έμπιστα μέρη κατά την εκτέλεση υπολογιστικών διεργασιών σε fog κόμβους [5].

Προηγμένες κρυπτογραφικές τεχνικές: ZKPs και ομομορφική κρυπτογράφηση.

Περαιτέρω ενίσχυση της ιδιωτικότητας επιτυγχάνεται μέσω της εφαρμογής προηγμένων κρυπτογραφικών τεχνικών, όπως οι αποδείξεις μηδενικής γνώσης (zero-knowledge proofs – ZKPs) και η ομομορφική κρυπτογράφηση (homomorphic encryption). Οι τεχνικές αυτές προσφέρουν τη δυνατότητα επεξεργασίας δεδομένων ή επαλήθευσης συναλλαγών χωρίς την αποκάλυψη του πραγματικού περιεχομένου των πληροφοριών [5]. Σε δημόσια ή κοινοπρακτικά δίκτυα, όπου η επικύρωση συναλλαγών και η συναίνεση απαιτούν κοινή επαλήθευση από πολλούς κόμβους, οι ZKPs επιτρέπουν να αποδειχθεί ότι μια συναλλαγή ή ένας κανόνας πολιτικής είναι έγκυρος, για παράδειγμα ότι ένας χρήστης έχει δικαίωμα πρόσβασης ή ότι μια ενέργεια τηρεί τους κανόνες, χωρίς να αποκαλύπτονται τα υποκείμενα δεδομένα. Στην περίπτωση αυτή, το blockchain προσφέρει το επιπλέον χαρακτηριστικό της κατανεμημένης και αμετάβλητης επαλήθευσης: όλοι οι κόμβοι μπορούν να ελέγξουν την ορθότητα της απόδειξης με ενιαίο τρόπο και το αποτέλεσμα της επαλήθευσης καταγράφεται με τρόπο ανιχνεύσιμο και μη αλλοιώσιμο, ενισχύοντας τη λογοδοσία σε περιβάλλοντα πολλών συμμετεχόντων [5].

Αντίστοιχα, η ομομορφική κρυπτογράφηση επιτρέπει την εκτέλεση υπολογισμών πάνω σε κρυπτογραφημένα δεδομένα, ώστε τα αποτελέσματα να προκύπτουν χωρίς να αποκαλύπτεται το αρχικό περιεχόμενο. Σε fog και edge σενάρια αυτό είναι ιδιαίτερα χρήσιμο όταν δεδομένα επεξεργάζονται από ενδιάμεσους κόμβους ή τρίτους φορείς. Στη σύζευξη αυτή, το blockchain λειτουργεί κυρίως ως μηχανισμός διακυβέρνησης και απόδειξης ορθής εκτέλεσης: μπορεί να καταγράφει ποιος ζήτησε ή εκτέλεσε έναν υπολογισμό, υπό ποιες πολιτικές και με ποια δικαιώματα, καθώς και να διασφαλίζει ότι το αποτέλεσμα που επιστρέφεται αντιστοιχεί σε συμφωνημένη διαδικασία, π.χ. μέσω καταγραφής hash δεσμεύσεων ή πολιτικών πρόσβασης που επιβάλλονται από smart contracts [5]. Έτσι, η κρυπτογραφική προστασία της εμπιστευτικότητας συνδυάζεται με ακεραιότητα, ιχνηλασιμότητα και λογοδοσία στη ροή επεξεργασίας.

Πρακτικοί περιορισμοί και κόστος υλοποίησης.

Παρά τα σημαντικά πλεονεκτήματα που προσφέρει ο συνδυασμός blockchain με προηγμένες κρυπτογραφικές τεχνικές, η προσέγγιση αυτή συνοδεύεται και από ουσιώδεις αδυναμίες σε επίπεδο πρακτικής υλοποίησης. Ειδικότερα, η ομομορφική κρυπτογράφηση χαρακτηρίζεται από υψηλό υπολογιστικό κόστος, ενώ οι αποδείξεις μηδενικής γνώσης (ZKPs) επιβαρύνουν το σύστημα με πρόσθετο κόστος παραγωγής και επαλήθευσης αποδείξεων [5]. Οι περιορισμοί αυτοί καθιστούν δυσκολότερη την υιοθέτησή τους σε περιβάλλοντα fog και edge computing, όπου οι διαθέσιμοι υπολογιστικοί πόροι και οι απαιτήσεις χαμηλής καθυστέρησης είναι συνήθως αυστηρά περιορισμένοι. Για τον λόγο αυτό, η αξιοποίησή τους εξετάζεται κυρίως σε εφαρμογές όπου η εμπιστευτικότητα είναι κρίσιμη, όπως στην επεξεργασία ιατρικών ή

χρηματοοικονομικών δεδομένων, και όπου το όφελος από την ενισχυμένη προστασία ιδιωτικότητας δικαιολογεί το πρόσθετο κόστος [5].

Ενδεικτικοί τομείς εφαρμογής.

Η πρακτική διάσταση των παραπάνω αποτυπώνεται εύγλωττα σε συγκεκριμένους τομείς εφαρμογής. Στον χώρο της υγείας, τα συστήματα edge computing χρησιμοποιούνται για την άμεση λήψη και ανάλυση δεδομένων από φορητές ιατρικές συσκευές, όπου η προστασία των προσωπικών ιατρικών δεδομένων είναι κρίσιμη. Σε τέτοια σενάρια, το blockchain αξιοποιείται κυρίως ως μηχανισμός ακεραιότητας, καταγραφής και ελέγχου πρόσβασης, επιτρέποντας την ιχνηλασιμότητα ενεργειών, δηλαδή ποιος ζήτησε ή έλαβε πρόσβαση, πότε και υπό ποιες προϋποθέσεις, καθώς και την επιβολή πολιτικών πρόσβασης με τρόπο που ενισχύει τη λογοδοσία. Έχουν προταθεί εφαρμογές όπου ο ασθενής διατηρεί κεντρικό ρόλο στον έλεγχο πρόσβασης στα δεδομένα του (patient-centric access control), ενώ παράλληλα διασφαλίζονται η ακεραιότητα και η εμπιστευτικότητα των ιατρικών πληροφοριών [7]. Με αυτόν τον τρόπο, η κατανεμημένη και ανιχνεύσιμη διαχείριση προσβάσεων ενισχύει την εμπιστοσύνη των χρηστών στα fog/edge δίκτυα, μειώνοντας τον κίνδυνο αθέμιτης επεξεργασίας ή μη εξουσιοδοτημένης διάθεσης ευαίσθητων δεδομένων.

Αντίστοιχα, στην αλυσίδα εφοδιασμού φαρμάκων, οι διαδικασίες ιχνηλάτησης προϊόντων σε edge περιβάλλοντα, όπως σημεία αποθήκευσης, διανομής ή logistics nodes, συνοδεύονται από αυστηρές απαιτήσεις προστασίας εμπορικά ευαίσθητων πληροφοριών. Σε αυτό το πλαίσιο, το blockchain χρησιμοποιείται ως ενιαίο, ανθεκτικό μητρώο ιχνηλασιμότητας, το οποίο επιτρέπει την αδιάλειπτη καταγραφή κρίσιμων γεγονότων, όπως μεταφορές, παραλαβές και αλλαγές κατάστασης προϊόντος, με τρόπο που είναι δύσκολο να αλλοιωθεί, ενισχύοντας την ακεραιότητα και τη διαφάνεια της εφοδιαστικής αλυσίδας [11]. Παράλληλα, η ιδιωτικότητα και η προστασία εμπορικών δεδομένων εξασφαλίζονται μέσω ελεγχόμενης πρόσβασης και κατάλληλων κρυπτογραφικών πρακτικών, όπως η αποθήκευση ευαίσθητων δεδομένων εκτός αλυσίδας και η καταγραφή on-chain μόνο δεικτών ή δεσμεύσεων ακεραιότητας. Έτσι, η διαφάνεια δεν αναιρεί την ιδιωτικότητα, αλλά συνυπάρχει με αυτήν μέσω επαληθευσιμότητας, ελέγχου και κρυπτογραφικής προστασίας.

Συνολική αποτίμηση και όρια της τεχνολογίας.

Από ένα ευρύτερο πρίσμα, η εφαρμογή του blockchain στο fog και edge computing μεταβάλλει τη θεώρηση περί ιδιωτικότητας, από μια κατάσταση εξάρτησης από την αξιοπιστία ενός κεντρικού διαχειριστή σε ένα μοντέλο όπου η εμπιστοσύνη εδράζεται στους αλγόριθμους συναίνεσης, στους κανόνες διακυβέρνησης και στις κρυπτογραφικές δικλείδες του κατανεμημένου καθολικού. Αυτή η θεμελιώδης μεταβολή επιτρέπει στους χρήστες να αισθάνονται μεγαλύτερη σιγουριά ότι η διαχείριση των προσωπικών τους δεδομένων τελεί υπό συνθήκες διαφάνειας, ελέγχου και ασφάλειας, χωρίς να απαιτείται τυφλή εμπιστοσύνη σε τρίτα μέρη.

Για συστηματικότερη αποτίμηση της συμβολής του blockchain στη διατήρηση της ιδιωτικότητας σε περιβάλλοντα fog και edge computing, δεν αρκεί η

καταγραφή μόνο των πλεονεκτημάτων και των ευκαιριών που προσφέρει. Όπως προκύπτει και από την προηγούμενη ανάλυση, εξακολουθούν να υφίστανται τόσο εγγενείς περιορισμοί της ίδιας της τεχνολογίας όσο και εξωτερικές απειλές που μπορούν να επηρεάσουν την αποτελεσματικότητά της. Για τον λόγο αυτό, ακολουθεί συνοπτική SWOT ανάλυση, η οποία αποτυπώνει τις δυνάμεις (Strengths), τις αδυναμίες (Weaknesses), τις ευκαιρίες (Opportunities) και τις απειλές (Threats) που σχετίζονται με την αξιοποίηση του blockchain για την προστασία της ιδιωτικότητας στα fog/edge περιβάλλοντα.

Η παραπάνω αποτίμηση καταδεικνύει ότι το blockchain μπορεί να αποτελέσει σημαντικό ενισχυτικό παράγοντα για τη διατήρηση της ιδιωτικότητας σε fog και edge περιβάλλοντα, χωρίς όμως να συνιστά από μόνο του πλήρη λύση. Η αποτελεσματικότητά του εξαρτάται από τον συνδυασμό του με κατάλληλους μηχανισμούς διαχείρισης εμπιστοσύνης, ελέγχου πρόσβασης, προστασίας μεταδεδομένων, ασφαλούς off-chain αποθήκευσης και κανονιστικής συμμόρφωσης.

Ανακεφαλαιώνοντας, το blockchain προσφέρει πολυδιάστατες λύσεις όσον αφορά τη διατήρηση της ιδιωτικότητας στο fog και edge computing, καθώς ενσωματώνει μηχανισμούς όπως η ψευδωνυμοποίηση, ο έλεγχος πρόσβασης, τα έξυπνα συμβόλαια και οι διαφοροποιήσεις μεταξύ δημόσιων, ιδιωτικών και κοινοπρακτικών blockchains καθώς και πιο προηγμένες τεχνικές, όπως οι αποδείξεις μηδενικής γνώσης και η ομομορφική κρυπτογράφηση. Αυτές οι προσεγγίσεις επιτρέπουν την ασφαλή επεξεργασία και διαμοιρασμό δεδομένων σε αποκεντρωμένα περιβάλλοντα, ενισχύοντας την εμπιστοσύνη των χρηστών και των οργανισμών που αξιοποιούν το fog και edge computing [4], [5], [7], [9], [11].

6. Προκλήσεις και Ερευνητικές Κατευθύνσεις Σχετιζόμενες με την Εφαρμογή του Blockchain σε Fog/Edge Περιβάλλοντα

Η ενσωμάτωση του blockchain σε περιβάλλοντα fog και edge computing, παρότι προσφέρει σημαντικά οφέλη ως προς την ασφάλεια, την ακεραιότητα, τη λογοδοσία και, υπό προϋποθέσεις, την ιδιωτικότητα, δεν πραγματοποιείται χωρίς τεχνικές, λειτουργικές και αρχιτεκτονικές δυσκολίες. Οι ιδιαιτερότητες των fog/edge συστημάτων — όπως οι περιορισμένοι υπολογιστικοί και ενεργειακοί πόροι, οι απαιτήσεις χαμηλής καθυστέρησης, η ετερογένεια των κόμβων και η δυναμική τοπολογία — καθιστούν την εφαρμογή των μηχανισμών blockchain πιο σύνθετη σε σχέση με συμβατικά, περισσότερο σταθερά κατανεμημένα περιβάλλοντα. Στόχος του παρόντος κεφαλαίου είναι να αναδείξει τις κυριότερες προκλήσεις και τους περιορισμούς που εμφανίζονται κατά την αξιοποίηση του blockchain σε fog/edge αρχιτεκτονικές, καθώς και να παρουσιάσει τις βασικές ερευνητικές κατευθύνσεις που προτείνονται στη βιβλιογραφία για την αντιμετώπιση ή τον μετριασμό τους. Με τον τρόπο αυτό, το κεφάλαιο λειτουργεί όχι μόνο ως καταγραφή υφιστάμενων προβλημάτων, αλλά και ως γέφυρα προς τις μελλοντικές εξελίξεις του πεδίου.

Για να αποσαφηνιστεί η δομή του παρόντος κεφαλαίου, ο Πίνακας 10: Αντιστοίχιση προκλήσεων με ερευνητικές κατευθύνσεις σε fog/edge-blockchain συνοψίζει τις βασικές προκλήσεις/περιορισμούς που προκύπτουν κατά την εφαρμογή τεχνολογιών blockchain σε περιβάλλοντα fog/edge και τις κύριες ερευνητικές κατευθύνσεις που προτείνονται για τον μετριασμό τους.

Με βάση αυτή τη χαρτογράφηση, το κεφάλαιο οργανώνεται ανά πρόκληση, ώστε κάθε υποενότητα να παρουσιάζει: (i) το πρόβλημα και τις επιπτώσεις του σε fog/edge σενάρια και (ii) τις σχετικές ερευνητικές κατευθύνσεις. Συγκεκριμένα, η Ενότητα 6.1 καλύπτει προκλήσεις απόδοσης και κατανάλωσης πόρων (throughput, latency, ενέργεια, αποθήκευση), ενώ η Ενότητα 6.2 καλύπτει προκλήσεις ασφάλειας και ιδιωτικότητας (51% attack, smart contract vulnerabilities, ιδιωτικότητα συναλλαγών, κβαντικοί κίνδυνοι).

Σημειώνεται ότι αρκετές κατευθύνσεις (π.χ. off-chain/L2, sharding, data minimization) είναι οριζόντιες και επηρεάζουν περισσότερες από μία προκλήσεις· γι’ αυτό και στον πίνακα εμφανίζονται επαναλαμβανόμενα, ενώ στο κείμενο γίνονται οι αντίστοιχες διασυνδέσεις.

Η ενσωμάτωση του blockchain σε περιβάλλοντα fog και edge computing, παρότι προσφέρει σημαντικά πλεονεκτήματα ως προς την ακεραιότητα, τη λογοδοσία, την αποκεντρωμένη διακυβέρνηση και, υπό προϋποθέσεις, την ενίσχυση της ασφάλειας και της ιδιωτικότητας, συνοδεύεται από μια σειρά τεχνικών, λειτουργικών και αρχιτεκτονικών προκλήσεων. Οι ιδιαιτερότητες των

fog/edge συστημάτων, όπως οι περιορισμένοι υπολογιστικοί και ενεργειακοί πόροι, οι απαιτήσεις χαμηλής καθυστέρησης, η ετερογένεια των κόμβων και η δυναμική τοπολογία του δικτύου, καθιστούν την εφαρμογή μηχανισμών blockchain περισσότερο απαιτητική σε σχέση με άλλα κατανεμημένα περιβάλλοντα. Στόχος του παρόντος κεφαλαίου είναι να αναδείξει αφενός τις βασικές προκλήσεις και τους περιορισμούς που εμφανίζονται κατά την εφαρμογή του blockchain σε fog/edge αρχιτεκτονικές και αφετέρου τις κυριότερες ερευνητικές κατευθύνσεις που έχουν προταθεί για την αντιμετώπιση ή τον μετριασμό τους. Για τη συνοπτική αποτύπωση αυτής της σχέσης, ο Πίνακας 9 παρουσιάζει αντιστοιχισμένα τα κύρια προβλήματα με τις αντίστοιχες τεχνικές ή ερευνητικές προσεγγίσεις που προτείνονται στη βιβλιογραφία.

Πίνακας 10: Αντιστοίχιση προκλήσεων με ερευνητικές κατευθύνσεις σε fog/edge-blockchain

Πρόκληση / περιορισμός	**Ερευνητικές κατευθύνσεις / τεχνικές μετριασμού**	**Υποενότητα**
Περιορισμένος ρυθμός διεκπεραίωσης (throughput)	• Ελαφρύτεροι μηχανισμοί συναίνεσης (PoS/DPoS/PoA) • Sharding • Layer-2 / off-chain (π.χ. channels, rollups) • Batching/aggregation σε fog επίπεδο	6.1.1
Καθυστέρηση συναλλαγών (latency)	• Fast-finality / leader-based παραγωγή blocks • Βελτιστοποίηση propagation & P2P topology • Ελαφρά πρωτόκολλα επικοινωνίας (MQTT/CoAP + DTLS/TLS optimizations) • Data-size minimization / compact formats / off-chain μεγάλα δεδομένα • Local finality + global settlement, fog-side aggregation • Βελτιστοποιήσεις εκτέλεσης/επεξεργασίας συναλλαγών • Deadline-aware scheduling • Hardware-aware acceleration • AI-assisted latency control	6.1.2
Υψηλή κατανάλωση ενέργειας / πόρων	• Μετάβαση από PoW σε PoS/DPoS/υβριδικά σχήματα • Adaptive consensus με σαφή thresholds • Architectural offloading (edge→fog) • Layer-2/off-chain & batching	6.1.3

	• Lightweight cryptography & adaptive node participation • Energy-aware scheduling / AI-assisted optimization	
Αυξανόμενες απαιτήσεις αποθήκευσης	• Pruning & archival nodes • Off-chain storage (π.χ. IPFS) + on-chain commitments • Υβριδική αποθήκευση (hybrid storage) • Sharding/partitioning • Role-based nodes (full/partial/light) • Proof-based validation (header-only) • Cryptographic compression techniques • On-demand retrieval & cold storage • Federated storage with erasure coding • Retention policies / cold storage / semantic minimization • Hybrid DLT models (non-blockchain ledgers)	6.1.4
Ευπάθειες σε 51% attack / συγκέντρωση ισχύος	• Multi-party / quorum-based validation • Υβριδικά PoW/PoS (διακριτοί ρόλοι) • Hierarchical trust (fog-specific) • Stake/role diversification • Incentive discouragement (penalties, slashing κ.λπ.) • Ανίχνευση ανωμαλιών στην κατανομή ισχύος	6.2.1
Κενά σε έξυπνα συμβόλαια	• Εργαλεία στατικής/δυναμικής ανάλυσης (π.χ. Mythril, Oyente) • Secure standards (ERC-20/777) & guidelines • Security-by-design, formal methods / formal verification, safe language & compiler choices, secure design patterns • Runtime προστασίες (guards, circuit breakers) • Upgradeable-contract safety & external dependency hardening • Beyond conventional testing (property-based & adversarial testing) • Runtime monitoring & on-chain defense	6.2.2

Ζητήματα ιδιωτικότητας συναλλαγών	• Zero-knowledge foundations (Zerocoin, zk-SNARKs) • Προχωρημένες αποδείξεις μηδενικής γνώσης (zk-STARKs, bulletproofs) • Privacy-preserving rollups (zk-Rollups) • Mixing & obfuscation techniques (CoinJoin, CoinShuffle, mixnets, tumblers) • Ring-based anonymity • Confidential Transactions (Pedersen commitments) • Address-level & network-layer privacy (διευθύνσεις, stealth τεχνικές, μείωση μεταδεδομένων) • Trusted Execution Environments (TEE) • Secure Multi-Party Computation (MPC/SMPC) • Application-layer encryption • Selective disclosure • Hybrid privacy-preserving architectures	6.2.3
Κίνδυνοι από κβαντικούς υπολογιστές	• Post-Quantum Cryptography (lattice-based, hash-based signatures) • Υβριδικά/μεταβατικά σχήματα (classical + PQC) • Τυποποίηση/standards (π.χ. NIST PQC) • Στρατηγική μετάβασης για υπάρχοντα δίκτυα	6.2.4

Με βάση αυτή τη χαρτογράφηση, το κεφάλαιο οργανώνεται ανά πρόκληση, ώστε κάθε υποενότητα να παρουσιάζει: (i) το πρόβλημα και τις επιπτώσεις του σε fog/edge σενάρια και (ii) τις σχετικές ερευνητικές κατευθύνσεις.

6.1 Προκλήσεις Απόδοσης & Κατανάλωσης Πόρων

Η εφαρμογή τεχνολογιών blockchain σε περιβάλλοντα fog και edge computing εγείρει ιδιαίτερες προκλήσεις σε επίπεδο απόδοσης και αξιοποίησης πόρων, καθώς τα περιβάλλοντα αυτά χαρακτηρίζονται από περιορισμένη υπολογιστική ισχύ, περιορισμένη αποθηκευτική ικανότητα, αυστηρές απαιτήσεις χαμηλής καθυστέρησης και, συχνά, περιορισμένο ενεργειακό προϋπολογισμό. Σε αντίθεση με πιο ισχυρές και σταθερές κεντρικές ή νεφοϋπολογιστικές υποδομές, τα fog/edge συστήματα καλούνται να διαχειριστούν μεγάλο όγκο

δεδομένων και συναλλαγών κοντά στην πηγή παραγωγής τους, γεγονός που καθιστά κρίσιμη τη διατήρηση ισορροπίας μεταξύ ασφάλειας, αποκέντρωσης και αποδοτικότητας. Στο πλαίσιο αυτό, η παρούσα ενότητα εξετάζει τις βασικές προκλήσεις που σχετίζονται με τον ρυθμό διεκπεραίωσης, την καθυστέρηση, την κατανάλωση ενέργειας και τις απαιτήσεις αποθήκευσης, καθώς και τις αντίστοιχες ερευνητικές κατευθύνσεις που διερευνώνται για την αντιμετώπισή τους.

6.1.1. Περιορισμένος ρυθμός διεκπεραίωσης συναλλαγών (throughput)

6.1.1.1 Ανάλυση Πρόκλησης

Μία από τις πλέον κρίσιμες προκλήσεις που αντιμετωπίζει η τεχνολογία του blockchain, ειδικά όταν καλείται να εφαρμοστεί σε κατανεμημένα περιβάλλοντα όπως το fog και το edge computing, αφορά τον περιορισμένο ρυθμό διεκπεραίωσης συναλλαγών (throughput). Ο όρος throughput περιγράφει τον αριθμό των συναλλαγών που μπορεί να επεξεργαστεί το σύστημα ανά μονάδα χρόνου. Στην περίπτωση των δημόσιων blockchains, όπως το Bitcoin, ο αριθμός αυτός είναι σημαντικά χαμηλός συγκριτικά με παραδοσιακές τραπεζικές πλατφόρμες ή κεντρικοποιημένα δίκτυα πληρωμών, γεγονός που αναδεικνύει τη δυσκολία ενσωμάτωσης του blockchain σε συστήματα πραγματικού χρόνου, όπως αυτά του fog και edge υπολογισμού [1], [4].

Η περιορισμένη δυνατότητα επεξεργασίας συναλλαγών αποδίδεται κυρίως στην αρχιτεκτονική του blockchain, η οποία βασίζεται σε ένα αποκεντρωμένο μηχανισμό συναίνεσης μεταξύ κόμβων. Στην περίπτωση του Bitcoin, εφαρμόζεται ο μηχανισμός Proof of Work (PoW), ο οποίος, αν και ενισχύει την ασφάλεια και την ακεραιότητα του δικτύου, συνεπάγεται μεγάλες καθυστερήσεις στην επικύρωση των συναλλαγών και στη δημιουργία νέων blocks. Ειδικότερα, η δημιουργία ενός block στο δίκτυο Bitcoin απαιτεί κατά μέσο όρο 10 λεπτά, γεγονός που οδηγεί σε χαμηλό ρυθμό διεκπεραίωσης, της τάξεως των 7 συναλλαγών ανά δευτερόλεπτο (transactions per second – TPS), ρυθμός που θεωρείται ανεπαρκής για εφαρμογές υψηλών απαιτήσεων, όπως η διαχείριση δεδομένων IoT σε fog ή edge περιβάλλοντα [1].

Παρόμοιοι περιορισμοί εντοπίζονται και σε άλλα δημόσια blockchains, όπως το Ethereum, το οποίο, παρά το γεγονός ότι υποστηρίζει έξυπνα συμβόλαια, αντιμετωπίζει χαμηλό throughput, περίπου 30 συναλλαγές ανά δευτερόλεπτο, λόγω της χρήσης του PoW μέχρι την πρόσφατη μετάβαση σε Proof of Stake (PoS) με το Ethereum 2.0 [5]. Η μειωμένη απόδοση καθιστά δυσχερή τη χρήση του blockchain ως υποδομής για συστήματα fog/edge computing, όπου απαιτείται ταχεία επικύρωση δεδομένων αισθητήρων και διασφάλιση της εγκυρότητας των επικοινωνιών μεταξύ των κόμβων.

Οι εφαρμογές fog και edge computing χαρακτηρίζονται από υψηλή διασύνδεση και αδιάλειπτη ροή δεδομένων, με αποτέλεσμα η καθυστέρηση που προκαλείται από τον περιορισμένο ρυθμό διεκπεραίωσης των blockchain συναλλαγών να επηρεάζει δυσμενώς την απόδοση των συστημάτων. Το ζήτημα επιδεινώνεται όταν απαιτείται η καταγραφή μεγάλου όγκου συναλλαγών σε σύντομο χρονικό διάστημα, όπως για παράδειγμα στην αδιάλειπτη

παρακολούθηση λειτουργικών παραμέτρων βιομηχανικών εγκαταστάσεων ή στην καταγραφή ιατρικών δεδομένων σε πραγματικό χρόνο.

6.1.1.2 Ερευνητικές Κατευθύνσεις

Η αντιμετώπιση του ζητήματος του περιορισμένου throughput αποτελεί αντικείμενο εντατικής ερευνητικής δραστηριότητας, με στόχο την ανάπτυξη λύσεων που θα επιτρέψουν την απρόσκοπτη ενσωμάτωση του blockchain σε περιβάλλοντα με αυξημένες απαιτήσεις ταχύτητας και απόδοσης.

Ελαφρύτεροι μηχανισμοί συναίνεσης (PoS / DPoS).

Ανάμεσα στις πλέον υποσχόμενες προσεγγίσεις συγκαταλέγεται *η αξιοποίηση ελαφρύτερων μηχανισμών συναίνεσης*, όπως ο Proof of Stake (PoS) και ο Delegated Proof of Stake (DPoS), οι οποίοι μειώνουν σημαντικά τον χρόνο επικύρωσης συναλλαγών, περιορίζοντας τη χρήση υπολογιστικών πόρων και ενισχύοντας την αποδοτικότητα των αποκεντρωμένων δικτύων. Ο PoS στηρίζεται στην επιλογή κόμβων με βάση το μερίδιό τους στο ψηφιακό νόμισμα, αποφεύγοντας τη διαδικασία επίλυσης πολύπλοκων μαθηματικών προβλημάτων που χαρακτηρίζει τον PoW. Αντίστοιχα, το DPoS επιτρέπει στους κατόχους tokens να εκλέγουν αντιπροσώπους, οι οποίοι αναλαμβάνουν τη δημιουργία blocks, επιτυγχάνοντας έτσι ταχύτερη συναίνεση [5].

Sharding

Ιδιαίτερο ενδιαφέρον παρουσιάζει *η ανάπτυξη τεχνικών sharding*, οι οποίες στοχεύουν στη διαίρεση του δικτύου σε μικρότερες, αυτόνομες ομάδες κόμβων (shards), κάθε μία από τις οποίες επεξεργάζεται ένα υποσύνολο συναλλαγών. Η προσέγγιση αυτή επιτρέπει την παράλληλη διεκπεραίωση συναλλαγών, αυξάνοντας δραστικά τον συνολικό ρυθμό επεξεργασίας και διασφαλίζοντας τη δυνατότητα κλιμάκωσης του συστήματος χωρίς να διακυβεύεται η αποκέντρωση [4].

Layer 2 / off-chain λύσεις

Περαιτέρω, προωθείται η υιοθέτηση λύσεων Layer 2, όπως το Lightning Network, το οποίο λειτουργεί ως επιπρόσθετο επίπεδο πάνω από το βασικό blockchain, επιτρέποντας τη διενέργεια μικρο-συναλλαγών εκτός αλυσίδας (off-chain). Οι συναλλαγές αυτές διεκπεραιώνονται απευθείας μεταξύ των συμμετεχόντων, χωρίς την ανάγκη καταγραφής τους στο δημόσιο ledger για κάθε μεμονωμένη πράξη. Το τελικό αποτέλεσμα των συναλλαγών ενσωματώνεται στο blockchain μόνο όταν ολοκληρωθεί η αλληλεπίδραση, μειώνοντας έτσι τον φόρτο στο κύριο δίκτυο και αυξάνοντας την απόδοση του συστήματος [1].

Batching και aggregation σε επίπεδο fog.

Μία ακόμη σημαντική ερευνητική κατεύθυνση αφορά τις τεχνικές batching και aggregation σε επίπεδο fog. Στην προσέγγιση αυτή, ενδιάμεσοι fog κόμβοι ή gateways συλλέγουν μεγάλο αριθμό μικρών συναλλαγών ή γεγονότων που παράγονται από edge συσκευές και τα ομαδοποιούν σε πιο συμπαγείς

εγγραφές, πριν από την προώθησή τους στο blockchain. Με τον τρόπο αυτό μειώνεται ο συνολικός αριθμός των συναλλαγών που πρέπει να επικυρωθούν και να καταγραφούν on-chain, περιορίζεται ο φόρτος του δικτύου και βελτιώνεται ο συνολικός ρυθμός διεκπεραίωσης. Η τεχνική αυτή είναι ιδιαίτερα χρήσιμη σε fog/edge περιβάλλοντα με μαζική παραγωγή τηλεμετρικών ή αισθητηριακών δεδομένων, όπου η απευθείας καταγραφή κάθε μεμονωμένου γεγονότος στο blockchain θα οδηγούσε σε συμφόρηση και αισθητή υποβάθμιση της απόδοσης.

Η συνέχιση της ερευνητικής δραστηριότητας προς την κατεύθυνση της βελτίωσης των παραπάνω τεχνολογιών, καθώς και η διερεύνηση νέων υβριδικών μοντέλων που συνδυάζουν off-chain και on-chain επεξεργασία δεδομένων, κρίνεται απαραίτητη για τη μελλοντική εξέλιξη των συστημάτων blockchain σε εφαρμογές fog και edge computing. Οι προσπάθειες αυτές αναμένεται να συμβάλουν στη διαμόρφωση μιας πιο ευέλικτης και αποδοτικής αρχιτεκτονικής, ικανής να ανταποκριθεί στις ιδιαίτερες απαιτήσεις των κατανεμημένων υπολογιστικών συστημάτων.

6.1.2. Ζητήματα Καθυστέρησης (latency)

6.1.2.1 Ανάλυση Πρόκλησης

Ένα από τα πλέον κρίσιμα προβλήματα που ανακύπτουν κατά την εφαρμογή τεχνολογιών blockchain σε περιβάλλοντα fog και edge computing είναι η καθυστέρηση στη μετάδοση και επικύρωση των συναλλαγών, γνωστή ως latency. Ο όρος αυτός αναφέρεται στον χρόνο που απαιτείται από τη στιγμή που μία συναλλαγή δημιουργείται έως την οριστική ενσωμάτωσή της στο blockchain. Η αυξημένη καθυστέρηση μπορεί να έχει αρνητικό αντίκτυπο στη λειτουργικότητα εφαρμογών που απαιτούν σχεδόν άμεση απόκριση, ιδίως σε κατανεμημένα δίκτυα όπως τα fog και edge, τα οποία συχνά καλούνται να υποστηρίξουν εφαρμογές πραγματικού χρόνου.

Η φύση των blockchains, ιδιαίτερα των δημόσιων, καθιστά τη διαδικασία επικύρωσης και ενσωμάτωσης νέων συναλλαγών συγκριτικά αργή. Στα πλαίσια μηχανισμών συναίνεσης όπως η Απόδειξη Εργασίας (Proof of Work), η εισαγωγή ενός block στην αλυσίδα απαιτεί την επίλυση πολύπλοκων υπολογιστικών γρίφων, διαδικασία που, αν και εξασφαλίζει υψηλά επίπεδα ασφάλειας, συνεπάγεται σημαντική καθυστέρηση [4]. Ακόμα και σε εναλλακτικά μοντέλα συναίνεσης, όπως η Απόδειξη Κατοχής (Proof of Stake), παρατηρούνται χρονικές υστερήσεις, ειδικά όταν το δίκτυο περιλαμβάνει μεγάλο αριθμό κόμβων ή βρίσκεται σε περιβάλλον με περιορισμένους υπολογιστικούς και δικτυακούς πόρους, όπως συμβαίνει σε υποδομές fog και edge [5].

Σε συνέχεια, το propagation time, δηλαδή ο χρόνος διάδοσης των πληροφοριών μεταξύ των κόμβων του δικτύου, αποτελεί έναν ακόμη παράγοντα που συμβάλλει στην αύξηση του latency. Όταν μια συναλλαγή μεταδίδεται σε ένα κατανεμημένο δίκτυο με γεωγραφικά απομακρυσμένους κόμβους ή όταν οι διαθέσιμες δικτυακές υποδομές παρουσιάζουν περιορισμένη

ταχύτητα, η καθυστέρηση στη μετάδοση των blocks μπορεί να οδηγήσει σε χρονικά κενά στην επικύρωση, επιβραδύνοντας τη συνολική απόδοση του συστήματος.

Οι επιπτώσεις του αυξημένου latency είναι ιδιαίτερα αισθητές σε εφαρμογές που βασίζονται σε fog και edge αρχιτεκτονικές, καθώς οι συγκεκριμένες υποδομές συχνά στοχεύουν στην παροχή υπηρεσιών με χαμηλή καθυστέρηση. Εφαρμογές όπως η παρακολούθηση συστημάτων υγείας, ο έλεγχος βιομηχανικών διεργασιών και η αυτόνομη οδήγηση απαιτούν άμεση απόκριση των συστημάτων, γεγονός που καθιστά τις καθυστερήσεις στις συναλλαγές blockchain ανασταλτικό παράγοντα για την ευρεία υιοθέτηση της τεχνολογίας αυτής στα συγκεκριμένα πεδία.

6.1.2.2 Ερευνητικές Κατευθύνσεις

Απέναντι στις προκλήσεις που εγείρει το latency, έχουν προταθεί διάφορες ερευνητικές κατευθύνσεις που αποσκοπούν στη μείωση του χρόνου που απαιτείται για τη μετάδοση και επικύρωση των συναλλαγών, καθιστώντας τις blockchain εφαρμογές περισσότερο αποδοτικές και κατάλληλες για χρήση σε fog και edge περιβάλλοντα [2], [3], [5], [17].

Για λόγους σαφήνειας, οι ερευνητικές κατευθύνσεις για τη μείωση του latency μπορούν να ομαδοποιηθούν σε πέντε επίπεδα: (i) μηχανισμοί συναίνεσης (consensus layer), (ii) διάδοση/επικοινωνία (network & propagation), (iii) εκτέλεση/επεξεργασία συναλλαγών (execution), (iv) αρχιτεκτονικές τεχνικές (architectural offloading) και (v) προγραμματισμός/προτεραιοποίηση (scheduling), με συμπληρωματικές βελτιστοποιήσεις που αφορούν μέγεθος δεδομένων και επιτάχυνση υλικού [3], [5], [17].

Consensus-layer latency reduction. Μία από τις πιο άμεσες προσεγγίσεις για τη μείωση του latency αφορά την επιτάχυνση της οριστικοποίησης (finality) και τη μείωση των γύρων συντονισμού που απαιτούνται για την επικύρωση blocks. Σε fog/edge περιβάλλοντα, η ανάγκη για γρήγορη επιβεβαίωση συναλλαγών είναι κρίσιμη, καθώς η καθυστέρηση δεν οφείλεται μόνο στον υπολογισμό αλλά και στις μεταβαλλόμενες συνθήκες δικτύου και στους περιορισμένους πόρους. Για τον λόγο αυτό, προτείνονται μηχανισμοί *fast-finality consensus* και σχήματα που μειώνουν το “παράθυρο αβεβαιότητας”, ώστε οι εφαρμογές πραγματικού χρόνου να βασίζονται σε ταχύτερα τελεσίδικες αποφάσεις [5], [22], [23], [24].

Leader-based block production & adaptive block parameters. Συμπληρωματικά, σχήματα όπου ο ρόλος παραγωγής blocks ανατίθεται προσωρινά σε εκλεγμένο κόμβο (leader) μπορούν να περιορίσουν το επικοινωνιακό κόστος συντονισμού, μειώνοντας το latency σε κατανεμημένες τοπολογίες. Παράλληλα, η δυναμική προσαρμογή παραμέτρων όπως συχνότητα παραγωγής blocks ή μέγεθος blocks (*adaptive block parameters*) επιτρέπει στο σύστημα να ανταποκρίνεται σε συμφόρηση ή περιορισμένο bandwidth, μειώνοντας καθυστερήσεις διάδοσης και συσσώρευσης ουρών συναλλαγών [5], [22], [23], [24].

Propagation optimization. Μία βασική προσέγγιση αφορά τη βελτιστοποίηση του propagation time μεταξύ των κόμβων του δικτύου. Η μείωση του χρόνου

διάδοσης μπορεί να επιτευχθεί μέσω της ανάπτυξης πιο αποτελεσματικών αλγορίθμων διάχυσης πληροφοριών, καθώς και της αναδιάρθρωσης των δικτύων peer-to-peer, ώστε να μειωθούν οι ενδιάμεσοι σταθμοί κατά τη μετάδοση των blocks [5]. Οι βελτιωμένες δομές γειτνίασης μεταξύ των κόμβων ενδέχεται να μειώσουν αισθητά τον χρόνο που απαιτείται για την επίτευξη συναίνεσης .

Lightweight communication protocols. Επιπρόσθετα, η χρήση αποδοτικότερων πρωτοκόλλων επικοινωνίας αποτελεί μια ακόμη υποσχόμενη κατεύθυνση. Η μετάβαση από παραδοσιακά πρωτόκολλα σε πιο ελαφριά και προσαρμοσμένα στις ανάγκες των fog και edge δικτύων επικοινωνιακά μοντέλα ενδέχεται να περιορίσει τη χρονική καθυστέρηση, χωρίς να διακυβεύεται η ασφάλεια και η αξιοπιστία των συναλλαγών. Ενδεικτικά, σε περιβάλλοντα IoT/fog/edge αξιοποιούνται συχνά πρωτόκολλα όπως το MQTT ή το CoAP, τα οποία είναι σχεδιασμένα για συσκευές περιορισμένων πόρων και ασταθείς συνδέσεις, μειώνοντας το overhead σε σχέση με πιο «βαριά» μοντέλα επικοινωνίας [2], [3], [17]. Παράλληλα, για την ασφάλεια σε τέτοια κανάλια χρησιμοποιούνται ελαφριότερες υλοποιήσεις όπως DTLS (ιδίως πάνω από UDP για CoAP) ή «ελαφρύ TLS» σε συνδυασμό με μηχανισμούς επαναχρησιμοποίησης συνεδρίας (session resumption), ώστε να περιορίζεται το κόστος χειραψίας και η καθυστέρηση χωρίς να θυσιάζεται η εμπιστευτικότητα και η ακεραιότητα.

Data-size minimization. Η μείωση του μεγέθους των συναλλαγών και των blocks αποτελεί επίσης κρίσιμη κατεύθυνση, καθώς ο χρόνος διάδοσης εξαρτάται άμεσα από το bandwidth και το συνολικό payload. Σε fog/edge περιβάλλοντα, όπου οι ασύρματες ζεύξεις και οι περιορισμένοι πόροι είναι συχνό φαινόμενο, η ελαχιστοποίηση μεταδεδομένων, η χρήση συμπαγών formats και η αποθήκευση μεγάλων δεδομένων εκτός αλυσίδας (με on-chain δείκτες/δεσμεύσεις ακεραιότητας) μπορεί να μειώσει σημαντικά τις καθυστερήσεις μετάδοσης, χωρίς να υποβαθμίζεται η δυνατότητα επαλήθευσης [4], [5].

Hybrid / permissioned blockchain architectures. Ιδιαίτερη έμφαση δίνεται στην ανάπτυξη υβριδικών blockchains, τα οποία συνδυάζουν χαρακτηριστικά από δημόσια και ιδιωτικά δίκτυα. Τα συστήματα αυτά επιτρέπουν τη διενέργεια ταχύτερων συναλλαγών μέσω των ιδιωτικών blockchains, διατηρώντας, ταυτόχρονα, τη διαφάνεια και την ασφάλεια των δημόσιων αλυσίδων, όπου απαιτείται [9], [10], [22], [23], [24]. Οι ιδιωτικοί κόμβοι μπορούν να λειτουργούν ως ενδιάμεσα επίπεδα που επικυρώνουν συναλλαγές με μικρότερη καθυστέρηση, πριν αυτές συγχωνευθούν σε ένα ευρύτερο δημόσιο blockchain για λόγους διαφάνειας και διασφάλισης της ακεραιότητας [4].

Local finality + global settlement. Τέλος, ορισμένες προσεγγίσεις εξετάζουν τη δημιουργία τοπικών subnetworks εντός των fog και edge υποδομών, όπου η συναίνεση επιτυγχάνεται τοπικά, χωρίς να απαιτείται κάθε συναλλαγή να διαχέεται σε ολόκληρο το δίκτυο. Τα subnetworks αυτά μπορούν να διατηρούν τοπικά αρχεία των συναλλαγών και να ενημερώνουν περιοδικά το βασικό blockchain, περιορίζοντας έτσι τον φόρτο επικοινωνίας και τις καθυστερήσεις. Η προσέγγιση αυτή αντιστοιχεί σε αρχιτεκτονικές *local finality + global settlement*, όπου επιτυγχάνεται άμεση τοπική οριστικοποίηση και περιοδική

ενοποίηση/εκκαθάριση σε ανώτερο επίπεδο, μειώνοντας το end-to-end latency σε fog/edge εφαρμογές [2], [3], [5], [17].

Fog-side transaction aggregation. Μια συγγενής τεχνική είναι η συγκέντρωση συναλλαγών σε ισχυρότερους ενδιάμεσους κόμβους (fog gateways ή micro-data centers), οι οποίοι λειτουργούν ως “aggregators” συλλέγοντας μικρές συναλλαγές από πολλαπλές edge συσκευές, πραγματοποιώντας προκαταρκτικούς ελέγχους και προωθώντας πιο συμπαγείς ομαδοποιημένες εγγραφές προς το δίκτυο. Με αυτόν τον τρόπο μειώνεται η πίεση στο mempool/consensus, περιορίζεται ο αριθμός μεταδιδόμενων μηνυμάτων και βελτιώνεται η απόδοση σε περιόδους υψηλού telemetry traffic [2], [3], [17].

Execution & processing optimizations. Ακόμη και όταν η διάδοση και η συναίνεση βελτιστοποιούνται, σημαντικό μέρος του latency προκύπτει από την επεξεργασία συναλλαγών σε ετερογενείς κόμβους fog/edge. Για τον λόγο αυτό εξετάζονται τεχνικές όπως *parallel transaction execution* (όπου επιτρέπεται από τη δομή της κατάστασης), καθώς και *pre-validation & speculative execution*, με στόχο να μειωθεί ο χρόνος από την υποβολή συναλλαγής μέχρι τη δέσμευσή της σε block. Παράλληλα, η χρήση *lightweight cryptography* και βελτιστοποιημένων ελέγχων υπογραφών/ακεραιότητας περιορίζει το υπολογιστικό κόστος σε κόμβους με περιορισμένους πόρους, συμβάλλοντας στη μείωση της συνολικής καθυστέρησης [5].

Scheduling & prioritization. Τέλος, σε fog/edge εφαρμογές πραγματικού χρόνου δεν έχουν όλες οι συναλλαγές την ίδια κρισιμότητα. Η αξιοποίηση *priority queues* και *deadline-aware scheduling* επιτρέπει την προνομιακή εξυπηρέτηση συναλλαγών με αυστηρά χρονικά όρια (π.χ. alarms, control messages), ώστε να διατηρείται η απαιτούμενη απόκριση ακόμη και σε συνθήκες συμφόρησης. Η κατεύθυνση αυτή βελτιώνει τη “χρηστική” καθυστέρηση (application-level latency), ακόμη κι αν το συνολικό φορτίο παραμένει υψηλό [2], [3], [17].

Supporting optimizations. Επιπρόσθετα, υποστηρικτικές κατευθύνσεις όπως *hardware-aware acceleration* (αξιοποίηση επιτάχυνσης/ισχυρότερων fog κόμβων για βαριές επαληθεύσεις), *latency-tolerant consistency models* (δηλαδή μοντέλα στα οποία δεν απαιτείται άμεση καθολική συμφωνία όλων των κόμβων για κάθε συναλλαγή, αλλά επιτρέπεται προσωρινή τοπική αποδοχή ή συγχρονισμός σε επίπεδο fog/edge και η πλήρης εναρμόνιση με το υπόλοιπο δίκτυο πραγματοποιείται μεταγενέστερα (deferred settlement)) και *AI-assisted latency control* (πρόβλεψη συμφόρησης και δυναμική ρύθμιση παραμέτρων, όπως συχνότητα blocks) μπορούν να συμβάλουν στη σταθεροποίηση της καθυστέρησης σε ρεαλιστικές συνθήκες fog/edge [3], [5], [17].

Υπό συνολική οπτική, η αντιμετώπιση του ζητήματος της καθυστέρησης προϋποθέτει πολύπλευρες στρατηγικές που καλύπτουν τόσο το επίπεδο συναίνεσης και διάδοσης, όσο και το επίπεδο εκτέλεσης και αρχιτεκτονικού offloading. Ο συνδυασμός αποδοτικότερης επικοινωνίας, βελτιστοποιημένης διάχυσης των blocks, πολυεπίπεδων αρχιτεκτονικών (local finality / aggregation) και κατάλληλου scheduling μπορούν να ενισχύσουν τη συμβατότητα των blockchains με τα fog και edge συστήματα, επιτρέποντας την υιοθέτηση της τεχνολογίας σε κρίσιμες εφαρμογές που απαιτούν άμεση επεξεργασία και ανταπόκριση [2], [3], [5], [17].

6.1.3. Υψηλή Κατανάλωση Ενέργειας

6.1.3.1 Ανάλυση Πρόκλησης

Η ενεργειακή αποδοτικότητα αποτελεί έναν από τους πιο καίριους προβληματισμούς που συνοδεύουν την εφαρμογή τεχνολογιών blockchain, ιδιαίτερα όταν αυτές ενσωματώνονται σε περιβάλλοντα κατανεμημένης υπολογιστικής ισχύος, όπως το fog και το edge computing. Η αυξημένη κατανάλωση ενέργειας προκύπτει κυρίως από τη χρήση αλγορίθμων συναίνεσης που απαιτούν σημαντικούς υπολογιστικούς πόρους, με χαρακτηριστικότερο παράδειγμα τον μηχανισμό Proof of Work (PoW) που χρησιμοποιείται στο δίκτυο Bitcoin [1].

Ο μηχανισμός PoW βασίζεται στην επίλυση υπολογιστικά απαιτητικών κρυπτογραφικών γρίφων, οι οποίοι έχουν ως στόχο την αποτροπή κακόβουλων ενεργειών και την επίτευξη συναίνεσης μεταξύ των κόμβων του δικτύου. Παρά το γεγονός ότι η συγκεκριμένη μέθοδος έχει καταστεί συνώνυμη με την ανθεκτικότητα και την αξιοπιστία του Bitcoin, συνοδεύεται από ένα σημαντικό μειονέκτημα: τη δυσανάλογα υψηλή ενεργειακή κατανάλωση. Οι εξορύκτες (miners) ανταγωνίζονται για την επίλυση του γρίφου και την προσθήκη νέου block στην αλυσίδα, διαδικασία που οδηγεί σε διαρκή λειτουργία ισχυρών υπολογιστικών συστημάτων και σε εκτεταμένη χρήση ηλεκτρικής ενέργειας [1]. Η ενεργειακή αυτή επιβάρυνση συνεπάγεται κατ' επέκταση και προβλήματα απόδοσης/αξιοποίησης πόρων, καθώς η συνεχής επίλυση γρίφων δεσμεύει υπολογιστική ισχύ (CPU/GPU/ASIC), αυξάνει τη θερμική φόρτιση και περιορίζει τη διαθεσιμότητα πόρων για τις υπόλοιπες λειτουργίες του συστήματος. Σε περιβάλλοντα fog και, ιδίως, edge computing, όπου οι κόμβοι διαθέτουν περιορισμένη ισχύ, μνήμη και ενεργειακό προϋπολογισμό, η υιοθέτηση PoW καθίσταται πρακτικά δυσχερής, καθώς μπορεί να οδηγήσει σε υποβάθμιση της ποιότητας υπηρεσίας (QoS), αυξημένη καθυστέρηση και ταχύτερη εξάντληση διαθέσιμης ενέργειας. Ως αποτέλεσμα, η έντονη κατανάλωση πόρων δεν αποτελεί μόνο περιβαλλοντικό/οικονομικό ζήτημα, αλλά και τεχνικό εμπόδιο για την κλιμάκωση και την ένταξη PoW-based blockchains σε αποκεντρωμένες υποδομές κοντά στην ακμή [1].

Στο πλαίσιο των σύγχρονων προσεγγίσεων, εκτιμάται ότι το ενεργειακό αποτύπωμα του Bitcoin υπερβαίνει εκείνο ολόκληρων κρατών, γεγονός που εγείρει εύλογες ανησυχίες σχετικά με τη βιωσιμότητα του μοντέλου PoW σε εφαρμογές fog και edge computing, όπου το χαμηλό ενεργειακό κόστος και η αποδοτικότητα συνιστούν πρωταρχικές απαιτήσεις [4]. Ο συνδυασμός blockchain και κατανεμημένων υπολογιστικών αρχιτεκτονικών καθιστά αναγκαία τη διατήρηση μιας λεπτής ισορροπίας μεταξύ ασφάλειας, αποκέντρωσης και χαμηλής ενεργειακής επιβάρυνσης, προκειμένου να διασφαλιστεί η λειτουργική βιωσιμότητα των συστημάτων.

Οι κόμβοι σε fog και edge υποδομές είναι συχνά ενεργειακά περιορισμένοι, καθώς στηρίζονται σε συσκευές με περιορισμένες υπολογιστικές δυνατότητες και χαμηλή κατανάλωση. Η εισαγωγή ενεργοβόρων διαδικασιών, όπως το PoW, μπορεί να εξαντλήσει τα διαθέσιμα ενεργειακά αποθέματα των κόμβων

αυτών, μειώνοντας τη διάρκεια ζωής τους και υπονομεύοντας τη σταθερότητα του συνολικού συστήματος. Το γεγονός αυτό καθιστά τη διερεύνηση εναλλακτικών προσεγγίσεων αδήριτη ανάγκη, ώστε να διασφαλιστεί η απρόσκοπτη λειτουργία των κατανεμημένων δικτύων χωρίς υπέρμετρη ενεργειακή επιβάρυνση [5].

6.1.3.2 Ερευνητικές Κατευθύνσεις

Προκειμένου να αντιμετωπιστεί η προαναφερθείσα πρόκληση, η επιστημονική κοινότητα έχει εστιάσει στη μετάβαση από τον ενεργοβόρο μηχανισμό PoW σε περισσότερο ενεργειακά αποδοτικούς αλγορίθμους συναίνεσης. Στην κορυφή αυτών των εναλλακτικών επιλογών βρίσκεται το Proof of Stake (PoS), ένας μηχανισμός ο οποίος επιλέγει τον κόμβο που θα επικυρώσει το επόμενο block με βάση την ποσότητα κρυπτονομισμάτων που διατηρεί και όχι βάσει της υπολογιστικής του ισχύος. Η συγκεκριμένη προσέγγιση εξαλείφει την ανάγκη για επίλυση πολύπλοκων γρίφων, οδηγώντας σε σημαντική μείωση της κατανάλωσης ενέργειας, διατηρώντας ωστόσο την ασφάλεια και την αποκεντρωμένη φύση του συστήματος [5].

Πέραν του PoS, ιδιαίτερο ενδιαφέρον παρουσιάζει και ο Delegated Proof of Stake (DPoS), στον οποίο οι συμμετέχοντες εκλέγουν ένα περιορισμένο σύνολο αντιπροσώπων ή επικυρωτών για την παραγωγή και επικύρωση blocks. Με τον τρόπο αυτό περιορίζεται περαιτέρω το υπολογιστικό και ενεργειακό κόστος της διαδικασίας συναίνεσης, ενώ ταυτόχρονα επιτυγχάνονται ταχύτεροι χρόνοι επικύρωσης και μεγαλύτερη αποδοτικότητα, χαρακτηριστικά ιδιαίτερα χρήσιμα σε περιβάλλοντα fog και edge computing με περιορισμένους πόρους [5].

Εκτός από τις παραπάνω προσεγγίσεις, έχει προταθεί και η εφαρμογή υβριδικών μηχανισμών συναίνεσης, οι οποίοι συνδυάζουν στοιχεία τόσο από το PoW όσο και από το PoS, με στόχο την επίτευξη ενός βέλτιστου σημείου ισορροπίας μεταξύ ενεργειακής αποδοτικότητας και ασφάλειας. Οι υβριδικές αυτές μέθοδοι επιδιώκουν να μειώσουν το ενεργειακό αποτύπωμα των blockchain συστημάτων, ενσωματώνοντας παράλληλα χαρακτηριστικά που διασφαλίζουν την ανθεκτικότητα απέναντι σε κακόβουλες επιθέσεις [4].

Προσαρμοστική συναίνεση. Σημαντικές είναι επίσης οι ερευνητικές προσπάθειες που εστιάζουν στην ανάπτυξη καινοτόμων μεθόδων προσαρμοζόμενης συναίνεσης (adaptive consensus), όπου ο αλγόριθμος προσαρμόζεται δυναμικά ανάλογα με το φορτίο του δικτύου και τους διαθέσιμους πόρους. Για παράδειγμα, σε περιόδους χαμηλής κίνησης, το σύστημα μπορεί να υιοθετεί ελαφρύτερους μηχανισμούς επικύρωσης, μειώνοντας την ενεργειακή κατανάλωση, ενώ σε περιόδους αυξημένης δραστηριότητας, να ενισχύει τις διαδικασίες ασφάλειας. Ωστόσο, η δυναμική αυτή προσαρμογή συνεπάγεται αναπόφευκτα έναν συμβιβασμό (trade-off): η επιλογή πιο αυστηρών διαδικασιών ασφάλειας σε περιόδους αυξημένης δραστηριότητας τείνει να αυξάνει την κατανάλωση υπολογιστικών πόρων και ενέργειας, ενώ μπορεί να επιφέρει και επιπλέον καθυστέρηση στην επικύρωση, οδηγώντας σε αισθητή υποβάθμιση της απόδοσης (throughput/latency) του συστήματος. Για τον λόγο αυτό, οι adaptive προσεγγίσεις είναι αποτελεσματικές

μόνο όταν συνοδεύονται από σαφείς πολιτικές ενεργοποίησης (π.χ. thresholds για φόρτο/συμφόρηση), μηχανισμούς αποφυγής αστάθειας (oscillation) και προτεραιοποίηση κρίσιμων συναλλαγών, ώστε η αύξηση ασφάλειας να εφαρμόζεται στοχευμένα και να μην ακυρώνει τα πλεονεκτήματα των fog/edge υποδομών σε πραγματικό χρόνο.

Architectural offloading. Πέρα από την αντικατάσταση του PoW, ιδιαίτερο ενδιαφέρον παρουσιάζουν προσεγγίσεις που αξιοποιούν την κατανεμημένη αρχιτεκτονική των fog/edge συστημάτων, αναθέτοντας διαφορετικές λειτουργίες του blockchain σε διαφορετικά επίπεδα του συστήματος. Σε ένα σχήμα architectural offloading, εργασίες που είναι ενεργοβόρες για αδύναμες edge συσκευές (π.χ. επαλήθευση πολλαπλών υπογραφών, διαχείριση state, αποθήκευση μεγάλου ιστορικού) μεταφέρονται σε ισχυρότερους fog κόμβους ή σε επιλεγμένους validators, ενώ οι edge συσκευές περιορίζονται σε ελαφρύτερες λειτουργίες (π.χ. παραγωγή/υπογραφή συναλλαγών και βασικούς ελέγχους). Με αυτό τον τρόπο μειώνεται το ενεργειακό φορτίο στην ακμή χωρίς να εγκαταλείπεται η αποκεντρωμένη λογική του συστήματος, καθώς ο ρόλος κατανέμεται πολυεπίπεδα αντί να συγκεντρώνεται σε ένα σημείο.

Layer-2 / off-chain mechanisms. Ακόμη πιο ουσιαστική μείωση ενεργειακού κόστους προκύπτει όταν μειώνεται ο αριθμός συναλλαγών που απαιτούν πλήρη on-chain επεξεργασία. Οι layer-2 and off-chain τεχνικές επιτρέπουν την εκτέλεση αλληλεπιδράσεων εκτός αλυσίδας και την καταγραφή στην αλυσίδα μόνο συνοπτικών αποτελεσμάτων ή αποδεικτικών ακεραιότητας. Έτσι, μειώνεται το consensus load, η αποθήκευση και η επικοινωνιακή δραστηριότητα στο βασικό επίπεδο, στοιχεία που συνδέονται άμεσα με κατανάλωση ενέργειας—ιδίως σε fog/edge υποδομές όπου το bandwidth και οι υπολογιστικοί πόροι είναι περιορισμένοι.

Data minimization & off-chaining. Συμπληρωματικά, η ελαχιστοποίηση δεδομένων (data-size minimization) συνδέεται άμεσα με την off-chain αποθήκευση: όσο μικρότερο είναι το payload που μεταδίδεται και αποθηκεύεται on-chain, τόσο χαμηλότερη είναι η κατανάλωση ενέργειας που σχετίζεται με μετάδοση, επαλήθευση και αποθήκευση. Σε fog/edge σενάρια, όπου η επικοινωνία είναι συχνά ασύρματη και οι κόμβοι έχουν περιορισμένη μνήμη, η καταγραφή μόνο των απολύτως απαραίτητων μεταδεδομένων/δεσμεύσεων ακεραιότητας αποτελεί κρίσιμη σχεδιαστική επιλογή.

Transaction batching & aggregation. Στην ίδια κατεύθυνση, τεχνικές transaction batching & aggregation συγκεντρώνουν πολλές μικρές συναλλαγές (π.χ. telemetry events από IoT/edge) σε λιγότερες, πιο συμπαγείς εγγραφές. Αυτό μπορεί να γίνεται σε fog gateways ή ενδιάμεσους κόμβους, οι οποίοι λειτουργούν ως aggregators, εκτελώντας προκαταρκτικούς ελέγχους και μειώνοντας το συνολικό πλήθος μηνυμάτων και blocks που πρέπει να παραχθούν/διαδοθούν. Η προσέγγιση αυτή περιορίζει τόσο την επικοινωνιακή ενέργεια (λιγότερες μεταδόσεις) όσο και την υπολογιστική (λιγότερες επαληθεύσεις), ενώ είναι ιδιαίτερα ταιριαστή σε περιβάλλοντα με μαζικές, μικρές συναλλαγές.

Lightweight cryptography. Η κρυπτογραφία (υπογραφές, hashing, έλεγχοι ακεραιότητας) αποτελεί αναγκαίο αλλά συχνά ενεργοβόρο κομμάτι της

λειτουργίας blockchain. Η χρήση lightweight cryptography και βελτιστοποιημένων υλοποιήσεων μειώνει το κόστος ανά συναλλαγή, καθιστώντας εφικτή την ασφαλή λειτουργία σε κόμβους περιορισμένων πόρων. Αν και δεν “αντικαθιστά” τη συναίνεση, μειώνει τη σωρευτική κατανάλωση ενέργειας που προκαλείται από μεγάλους όγκους επαληθεύσεων, ιδίως σε edge περιβάλλοντα.

Adaptive node participation. Επιπλέον, ερευνητικές προσπάθειες εξετάζουν στρατηγικές adaptive node participation, όπου δεν συμμετέχουν όλοι οι κόμβοι με τον ίδιο τρόπο/ένταση σε όλες τις φάσεις του πρωτοκόλλου. Για παράδειγμα, επιλεγμένο υποσύνολο κόμβων μπορεί να αναλαμβάνει ρόλους επικύρωσης (validation) ή αποθήκευσης πλήρους ιστορικού, ενώ οι υπόλοιποι λειτουργούν ως light nodes. Έτσι, μειώνεται η ενεργειακή κατανάλωση συνολικά, χωρίς να απαιτείται κάθε συσκευή να εκτελεί πλήρεις και ενεργοβόρες λειτουργίες.

Hardware-aware acceleration. Άλλη γραμμή έρευνας αφορά hardware-aware optimization, δηλαδή τη βελτιστοποίηση με βάση το υλικό. Σε πολυεπίπεδες υποδομές fog/edge, μπορεί να αξιοποιηθούν ισχυρότεροι fog κόμβοι ή ειδικές δυνατότητες επιτάχυνσης (όπου υπάρχουν) για εντατικές εργασίες, ενώ οι χαμηλής ισχύος συσκευές περιορίζονται σε ελαφριά καθήκοντα. Η προσέγγιση αυτή δεν μειώνει μόνο την κατανάλωση, αλλά βελτιώνει και τη θερμική/λειτουργική σταθερότητα των edge κόμβων.

Energy-aware scheduling & orchestration. Σημαντικό ρόλο παίζουν και πολιτικές energy-aware scheduling & orchestration, όπου η ανάθεση εργασιών blockchain (επικυρώσεις, aggregations, αποθήκευση) γίνεται λαμβάνοντας υπόψη ενεργειακούς δείκτες (battery level, θερμική φόρτιση, τρέχον φορτίο). Με αυτόν τον τρόπο, αποφεύγεται η εξάντληση συγκεκριμένων κόμβων και διατηρείται η λειτουργική βιωσιμότητα του συστήματος σε βάθος χρόνου, κάτι κρίσιμο για edge συσκευές σε μη επιτηρούμενα περιβάλλοντα.

AI-assisted optimization. Τέλος, εξετάζονται προσεγγίσεις AI-assisted optimization για δυναμική προσαρμογή παραμέτρων με βάση προβλέψεις φόρτου και διαθέσιμων πόρων. Ενδεικτικά, το σύστημα μπορεί να προσαρμόζει δυναμικά μέγεθος/συχνότητα blocks, το σύνολο συμμετεχόντων στη συναίνεση ή τους ρόλους επικύρωσης, ώστε να επιτυγχάνεται ισορροπία μεταξύ ασφάλειας, απόδοσης και ενεργειακής κατανάλωσης. Η αξία αυτής της κατεύθυνσης σε fog/edge είναι ότι μπορεί να μετριάζει τις διακυμάνσεις των πόρων, διατηρώντας σταθερή συμπεριφορά χωρίς υπερβολικό ενεργειακό κόστος.

Υπό συνολική οπτική, η προσαρμογή των blockchain πρωτοκόλλων στις ιδιαίτερες απαιτήσεις ενεργειακής αποδοτικότητας των fog και edge περιβαλλόντων, αποτελεί πεδίο ιδιαίτερου επιστημονικού ενδιαφέροντος. Οι ερευνητικές προσπάθειες επικεντρώνονται στη διαμόρφωση σε όχι μόνο ελαφρύτερων και περισσότερο ευέλικτων μηχανισμών συναίνεσης αλλά και σε πολυεπίπεδες αρχιτεκτονικές και τεχνικές offloading/off-chain, ικανών να ανταποκριθούν στις απαιτήσεις των αποκεντρωμένων υπολογιστικών υποδομών, χωρίς να θέτουν σε κίνδυνο τις θεμελιώδεις αρχές της ασφάλειας και της αξιοπιστίας.

6.1.4. Αυξανόμενες Απαιτήσεις Αποθήκευσης

6.1.4.1 Ανάλυση Πρόκλησης

Η διαρκώς αυξανόμενη χωρητικότητα που απαιτείται για την αποθήκευση των δεδομένων σε blockchain υποδομές συνιστά μια από τις πλέον σύνθετες προκλήσεις, ειδικότερα σε περιβάλλοντα fog και edge computing, όπου οι διαθέσιμοι αποθηκευτικοί πόροι είναι συνήθως περιορισμένοι. Οι αρχιτεκτονικές αυτών των κατανεμημένων δικτύων στηρίζονται σε κόμβους που συχνά στερούνται επαρκούς αποθηκευτικού χώρου, γεγονός που καθιστά δυσχερή τη φιλοξενία του διαρκώς αυξανόμενου όγκου των blockchains [4].

Στο πλαίσιο της αποκεντρωμένης φύσης των blockchains, κάθε κόμβος καλείται να διατηρεί αντίγραφο ολόκληρης της αλυσίδας συναλλαγών (full node), διασφαλίζοντας με αυτόν τον τρόπο τη διαφάνεια, την ανθεκτικότητα και την ακεραιότητα του συστήματος. Καθώς, όμως, το blockchain εξελίσσεται με την πάροδο του χρόνου, ο όγκος των δεδομένων που απαιτείται να αποθηκευτεί αυξάνεται ραγδαία, δημιουργώντας ασφυκτικές πιέσεις στους κόμβους που λειτουργούν σε ενεργειακά και αποθηκευτικά περιορισμένα περιβάλλοντα [5]. Ιδιαίτερα σε εφαρμογές fog και edge υπολογιστικής, οι οποίες αξιοποιούν συσκευές με περιορισμένες δυνατότητες, η μακροπρόθεσμη διατήρηση του πλήρους ιστορικού των συναλλαγών μπορεί να υπερβεί τις φυσικές δυνατότητες των κόμβων, οδηγώντας σε μείωση της απόδοσης ή και σε εγκατάλειψη του δικτύου από μικρότερες μονάδες.

Επιπροσθέτως, στις περιπτώσεις των δημόσιων blockchain, όπως το Bitcoin, το μέγεθος της αλυσίδας αυξάνεται συνεχώς, υπερβαίνοντας ήδη το εύρος που μπορεί να διαχειριστεί μια συνηθισμένη υποδομή edge ή fog [5]. Οι απαιτήσεις αυτές επιτείνονται ακόμη περισσότερο σε περιβάλλοντα που απαιτούν υψηλές ταχύτητες συναλλαγών και αυξημένο αριθμό χρηστών, καθώς η αύξηση της χρήσης οδηγεί σε συχνότερη δημιουργία νέων blocks και, κατά συνέπεια, σε περαιτέρω διόγκωση του αποθηκευτικού κόστους.

Ενισχύοντας τις ανησυχίες, σε δημόσια blockchains, η ανάγκη για κάθε κόμβο να διαθέτει πλήρη πρόσβαση στο ιστορικό όλων των συναλλαγών ενδέχεται να λειτουργήσει ανασταλτικά για την υιοθέτηση των τεχνολογιών αυτών από μικρότερες επιχειρήσεις ή φορείς, οι οποίοι δεν διαθέτουν τους αναγκαίους αποθηκευτικούς και υπολογιστικούς πόρους [9]. Οι ιδιωτικές και consortium blockchain εκδόσεις παρουσιάζουν ελαφρώς μικρότερες απαιτήσεις, ωστόσο, και σε αυτές τις περιπτώσεις, το πρόβλημα της αποθήκευσης αναδεικνύεται σε καίριο ζήτημα, ειδικά όταν τα δεδομένα περιλαμβάνουν λεπτομερείς εγγραφές συναλλαγών, καταγραφές αισθητήρων ή αρχεία συμβάντων από δικτυακές υποδομές fog και edge.

6.1.4.2 Ερευνητικές Κατευθύνσεις

Block pruning. Στη διεθνή βιβλιογραφία έχουν προταθεί ερευνητικές προσεγγίσεις που στοχεύουν στον περιορισμό των απαιτήσεων αποθήκευσης χωρίς να υπονομεύεται η ασφάλεια και η διαφάνεια που χαρακτηρίζουν τα

blockchain δίκτυα. Μία από τις πλέον διαδεδομένες μεθόδους είναι η τεχνική του pruning, κατά την οποία παλαιότερα blocks, των οποίων οι συναλλαγές έχουν οριστικά επικυρωθεί και δεν χρήζουν περαιτέρω αναφοράς, αφαιρούνται από τοπικά αποθηκευμένες βάσεις δεδομένων των κόμβων. Όμως, αντί της πλήρους διαγραφής των blocks, διατηρούνται μόνο τα απαραίτητα hashes που επιβεβαιώνουν την ακεραιότητα του ιστορικού. Η πρακτική αυτή μειώνει τον συνολικό αποθηκευτικό χώρο που απαιτείται από τους κόμβους, καθιστώντας το blockchain πιο προσιτό σε περιβάλλοντα με περιορισμένους πόρους, όπως οι fog και edge αρχιτεκτονικές [5]. Σημειώνεται ότι το pruning δεν συνεπάγεται κατ' ανάγκη μεταφορά των ιστορικών δεδομένων σε κάποιο άλλο μέσο (π.χ. νέφος), αλλά κυρίως ότι ο εκάστοτε κόμβος παύει να διατηρεί πλήρες το ιστορικό τοπικά. Συνήθως, το πλήρες αρχείο (archival history) εξακολουθεί να διατηρείται από ένα υποσύνολο κόμβων του δικτύου ή από ειδικούς "archival" κόμβους, ενώ οι pruned κόμβοι κρατούν τα απαραίτητα δομικά στοιχεία/δεσμεύσεις (hashes, headers ή/και την τρέχουσα κατάσταση) για να μπορούν να λειτουργούν και να επαληθεύουν την ακεραιότητα. Παρ' όλα αυτά, σε εφαρμογές fog/edge όπου απαιτούνται μακροχρόνιες καταγραφές για συμμόρφωση ή αναλυτική επεξεργασία, είναι δυνατόν το πλήρες ιστορικό να αποθηκεύεται και εκτός αλυσίδας (π.χ. σε υποδομές cloud), με το blockchain να διατηρεί μόνο δείκτες/δεσμεύσεις ακεραιότητας [5].

Off-chain storage. Μία εναλλακτική κατεύθυνση που έχει λάβει ιδιαίτερη βαρύτητα τα τελευταία χρόνια είναι η αξιοποίηση συστημάτων αποθήκευσης εκτός της αλυσίδας (off-chain storage). Σύμφωνα με αυτή την προσέγγιση, ο κύριος όγκος των δεδομένων διατηρείται εκτός του blockchain, σε εξωτερικές αποκεντρωμένες ή κεντρικές αποθηκευτικές πλατφόρμες, ενώ στο blockchain ενσωματώνονται μόνο τα hashes των αρχείων. Με τον τρόπο αυτό, διασφαλίζεται η ακεραιότητα των δεδομένων μέσω των hashes, ενώ μειώνεται δραστικά το φορτίο αποθήκευσης στους κόμβους [4].

InterPlanetary File System (IPFS). Μία από τις πλέον καινοτόμες τεχνολογίες που υποστηρίζει την off-chain αποθήκευση είναι το InterPlanetary File System (IPFS), ένα πρωτόκολλο διαμοιρασμένης αποθήκευσης που αξιοποιεί τεχνικές κατανεμημένης ευρετηρίασης και δρομολόγησης περιεχομένου. Το IPFS επιτρέπει την αποθήκευση μεγάλων αρχείων σε αποκεντρωμένους κόμβους, ενώ η επαλήθευση της ακεραιότητάς τους πραγματοποιείται μέσω μοναδικών κρυπτογραφικών αναγνωριστικών. Η σύζευξη blockchain και IPFS αναμένεται να συμβάλει καθοριστικά στη μείωση του αποθηκευτικού φόρτου που επωμίζονται οι κόμβοι, διατηρώντας παράλληλα τα πλεονεκτήματα της αποκεντρωμένης και ασφαλούς καταγραφής δεδομένων [5].

Υβριδική Αποθήκευση. Μία ακόμα ερευνητική προοπτική επικεντρώνεται στη δημιουργία συστημάτων υβριδικής αποθήκευσης, στα οποία τα δεδομένα χωρίζονται ανάλογα με τη σημασία και την ευαισθησία τους. Οι κρίσιμες συναλλαγές διατηρούνται on-chain, διασφαλίζοντας τη διαφάνεια και την αμετάβλητη φύση τους, ενώ δευτερεύοντα ή λιγότερο ευαίσθητα δεδομένα αποθηκεύονται off-chain, σε πιο ευέλικτες και αποδοτικές αποθηκευτικές δομές.

Πέρα από τις προσεγγίσεις pruning και off-chain/hybrid αποθήκευσης, η βιβλιογραφία προτείνει και συμπληρωματικές τεχνικές κλιμάκωσης που

μειώνουν τις απαιτήσεις αποθήκευσης είτε μέσω καταμερισμού του καθολικού (ledger) σε τμήματα, είτε μέσω διαφοροποίησης του ρόλου των κόμβων, είτε μέσω συμπίεσης/ελαχιστοποίησης των δεδομένων και πολιτικών διατήρησης, ώστε να καθίσταται εφικτή η συμμετοχή ακόμη και κόμβων περιορισμένων πόρων σε fog και edge υποδομές.

Sharding & ledger partitioning. Μία επιπλέον κατεύθυνση που προτείνεται για τη μείωση των αποθηκευτικών απαιτήσεων είναι ο κατακερματισμός της αλυσίδας (sharding) ή γενικότερα το *ledger partitioning*, όπου ο καθολικός λογιστικός χώρος δεν αποθηκεύεται ως ενιαίο σώμα από όλους τους κόμβους, αλλά χωρίζεται σε τμήματα (shards/partitions). Κάθε κόμβος ή ομάδα κόμβων διατηρεί μόνο ένα υποσύνολο του συνολικού ιστορικού ή/και της κατάστασης, μειώνοντας δραστικά το storage ανά κόμβο. Η προσέγγιση είναι ιδιαίτερα ελκυστική σε fog/edge, καθώς επιτρέπει οι περιορισμένοι κόμβοι να συμμετέχουν χωρίς να φιλοξενούν ολόκληρο το ledger, αν και αυξάνει την πολυπλοκότητα διασταυρούμενων συναλλαγών και απαιτεί προσεκτικό σχεδιασμό για να μη θίγεται η συνολική συνέπεια και η ασφάλεια.

Federated storage with erasure coding. Για αποκεντρωμένες αποθηκευτικές λύσεις, μία επιπλέον κατεύθυνση είναι η *ομοσπονδιακή αποθήκευση* με *erasure coding*, όπου τα δεδομένα τεμαχίζονται και αποθηκεύονται ως πλεονάζοντα “θραύσματα” σε πολλούς κόμβους. Έτσι, αυξάνεται η ανθεκτικότητα χωρίς να απαιτείται πλήρης αντιγραφή (replication) παντού, μειώνοντας το συνολικό storage overhead. Τέτοιες τεχνικές ταιριάζουν σε fog οικοσυστήματα, όπου υπάρχουν πολλοί ενδιάμεσοι κόμβοι που μπορούν να μοιραστούν το αποθηκευτικό φορτίο.

Role/level-based node differentiation. Ιδιαίτερα συμβατή με fog/edge αρχιτεκτονικές είναι και η *διαφοροποίηση ρόλων κόμβων* ανάλογα με το επίπεδο/είδος συσκευής (edge vs fog vs cloud). Σε ένα *role/level-based* μοντέλο, οι ισχυρότεροι fog κόμβοι ή/και cloud υποδομές μπορούν να λειτουργούν ως “archival/full” nodes που διατηρούν μεγαλύτερο μέρος του ιστορικού, ενώ οι edge συσκευές υλοποιούν light λειτουργία, κρατώντας μόνο ό,τι είναι αναγκαίο (π.χ. headers, τρέχουσα κατάσταση, ή επιλεγμένα snapshots). Έτσι το συνολικό δίκτυο διατηρεί πλήρη επαληθευσιμότητα, αλλά δεν απαιτείται από κάθε edge κόμβο να επωμιστεί το πλήρες αποθηκευτικό κόστος.

Header-only and proof-based validation. Μια πιο “ελαφριά” μορφή συμμετοχής είναι η *επικύρωση βάσει αποδεικτικών* αντί πλήρους ιστορικού. Σε αυτή την προσέγγιση, ένας κόμβος μπορεί να αποθηκεύει μόνο τα headers των blocks και να επαληθεύει συγκεκριμένες συναλλαγές μέσω αποδεικτικών ένταξης (π.χ. Merkle proofs) που του παρέχονται κατά περίπτωση. Με αυτόν τον τρόπο μειώνεται σημαντικά ο αποθηκευτικός φόρτος σε edge κόμβους, ενώ η ακεραιότητα μπορεί να διατηρηθεί αφού οι αποδείξεις συνδέονται κρυπτογραφικά με τα headers και την αλυσίδα. Το trade-off είναι ότι απαιτείται μηχανισμός ανάκτησης αποδεικτικών/δεδομένων από άλλους κόμβους, άρα εισάγεται εξάρτηση από τη διαθεσιμότητα “πλουσιότερων” κόμβων.

Cryptographic compression techniques. Στη διεθνή έρευνα συναντώνται και τεχνικές *κρυπτογραφικής συμπίεσης*, όπου το ιστορικό ή/και μεγάλες δομές

κατάστασης δεν διατηρούνται αυτούσιες, αλλά αντικαθίστανται από πιο συμπαγείς κρυπτογραφικές δεσμεύσεις (commitments) ή συνοπτικά αποδεικτικά ορθότητας/ακεραιότητας. Η λογική είναι να μειωθεί το αποθηκευτικό αποτύπωμα, διατηρώντας όμως τη δυνατότητα επαλήθευσης (είτε για συγκεκριμένα γεγονότα είτε για συνολικές ιδιότητες του ledger). Στην πράξη, τέτοιες προσεγγίσεις είναι πιο κατάλληλες όταν το ζητούμενο είναι η επαληθευσιμότητα και όχι η άμεση πρόσβαση στο πλήρες ιστορικό σε κάθε κόμβο.

Time-limited and ephemeral blockchains. Σε ορισμένα fog/edge σενάρια, ειδικά σε τηλεμετρία ή σε εφαρμογές όπου ενδιαφέρει κυρίως η πρόσφατη κατάσταση, προτείνεται η χρήση *time-limited/ephemeral* αλυσίδων. Εκεί διατηρείται ένα "παράθυρο" πρόσφατων blocks (sliding window), ενώ το παλαιότερο ιστορικό αρχειοθετείται ή αντικαθίσταται από checkpoints/δεσμεύσεις. Η προσέγγιση αυτή μειώνει δραστικά το on-device storage και είναι ρεαλιστική όταν υπάρχουν σαφείς απαιτήσεις διατήρησης (retention) και το πλήρες ιστορικό δεν χρειάζεται να βρίσκεται μόνιμα διαθέσιμο στο edge.

Semantic data minimization (event abstraction & delta recording). Μία λιγότερο "πρωτοκολλιακή" αλλά πολύ πρακτική κατεύθυνση είναι η *σημασιολογική ελαχιστοποίηση δεδομένων*: αντί να αποθηκεύονται ωμές, λεπτομερείς καταγραφές (π.χ. συνεχές sensor stream), καταγράφονται αφαιρέσεις γεγονότων (event abstraction), σύνοψη/aggregates ή μόνο οι μεταβολές (deltas) μεταξύ διαδοχικών καταστάσεων. Έτσι, το ledger διατηρεί την πληροφορία που είναι επιχειρησιακά χρήσιμη και επαληθεύσιμη, χωρίς να "φουσκώνει" από υψηλής συχνότητας δεδομένα χαμηλής αξίας για μακροχρόνια αποθήκευση.

Compression-aware blockchain encoding. Συμπληρωματικά, η *compression-aware encoding* προσέγγιση στοχεύει στο να σχεδιάζεται ο τρόπος κωδικοποίησης των blocks/συναλλαγών ώστε να συμπιέζεται αποδοτικά (π.χ. λιγότερη πλεονάζουσα πληροφορία, πιο συμπαγή πεδία, αποφυγή επαναλήψεων). Αυτό δεν αλλάζει απαραίτητα τη λογική του blockchain, αλλά μειώνει το storage footprint "εκ φύσεως" και διευκολύνει ιδιαίτερα fog/edge εγκαταστάσεις όπου ο δίσκος/flash είναι περιορισμένος.

On-demand retrieval & cold storage. Άλλη πρακτική προσέγγιση είναι η *on-demand ανάκτηση* ιστορικών δεδομένων, σε συνδυασμό με *cold storage*. Οι edge/fog κόμβοι διατηρούν το "λειτουργικά απαραίτητο" υποσύνολο (π.χ. πρόσφατα δεδομένα, snapshots, headers), ενώ το παλαιό ιστορικό μεταφέρεται σε αρχειοθετημένα μέσα χαμηλού κόστους. Όταν απαιτηθεί (audit, dispute resolution), γίνεται ανάκτηση κατά ζήτηση. Το trade-off είναι ότι αυξάνεται ο χρόνος πρόσβασης στο παλιό ιστορικό, αλλά μειώνεται πολύ το μόνιμο κόστος αποθήκευσης στους κόμβους ακμής.

Application-layer retention policies. Εξίσου σημαντικές είναι οι *πολιτικές διατήρησης σε επίπεδο εφαρμογής* (retention policies). Σε πολλά σενάρια fog/edge, δεν είναι αναγκαίο (ούτε επιθυμητό) να αποθηκεύονται όλα τα δεδομένα επ' αόριστον. Με σαφείς πολιτικές (π.χ. χρονικά όρια, κατηγορίες δεδομένων, νομικές απαιτήσεις), το σύστημα μπορεί να κρατά on-chain μόνο

τα κρίσιμα στοιχεία και να αρχειοθετεί/αποσύρει τα υπόλοιπα, μειώνοντας διαρκώς το storage pressure χωρίς να θίγεται η λειτουργική αξία του ledger.

Hybrid DLT models (non-blockchain ledgers). Τέλος, αναφέρονται και *υβριδικά μοντέλα DLT* που δεν βασίζονται αποκλειστικά στη "γραμμική" δομή blockchain, αλλά υιοθετούν εναλλακτικούς μηχανισμούς καταγραφής/συμφωνίας (non-blockchain ledgers). Ο στόχος είναι να επιτευχθεί κατανεμημένη επαληθευσιμότητα με διαφορετικά trade-offs σε αποθήκευση, διάδοση και συνέπεια. Αυτή η κατεύθυνση είναι χρήσιμη όταν το κλασικό blockchain αποδεικνύεται υπερβολικά "βαρύ" για edge συστήματα, αν και η επιλογή του μοντέλου απαιτεί προσεκτική αξιολόγηση ως προς τις εγγυήσεις ασφάλειας και τη συμβατότητα με τις απαιτήσεις της εφαρμογής.

Αθροιστικά, οι παραπάνω ερευνητικές διαδρομές συνιστούν καθοριστικά βήματα προς την κατεύθυνση της διαμόρφωσης ενός βιώσιμου μοντέλου blockchain, προσαρμοσμένου στις ανάγκες των fog και edge υποδομών, όπου οι απαιτήσεις για περιορισμό των αποθηκευτικών αναγκών αποκτούν κομβική σημασία για την αδιάλειπτη και αποδοτική λειτουργία των αποκεντρωμένων δικτύων.

6.2. Προκλήσεις Ασφάλειας και Ιδιωτικότητας

Η εφαρμογή του blockchain σε περιβάλλοντα fog και edge computing δεν εγείρει μόνο ζητήματα απόδοσης και αξιοποίησης πόρων, αλλά και κρίσιμες προκλήσεις που σχετίζονται με την ασφάλεια και την ιδιωτικότητα. Η κατανεμημένη φύση των αρχιτεκτονικών αυτών, η ετερογένεια των κόμβων, η απουσία ενιαίου σημείου ελέγχου και η διαχείριση ευαίσθητων δεδομένων σε δυναμικά περιβάλλοντα αυξάνουν την επιφάνεια επίθεσης και καθιστούν αναγκαία την προσεκτική αξιολόγηση των σχετικών κινδύνων. Στο πλαίσιο αυτό, η παρούσα ενότητα εξετάζει βασικές προκλήσεις όπως οι επιθέσεις 51%, οι ευπάθειες των έξυπνων συμβολαίων, τα ζητήματα ιδιωτικότητας των συναλλαγών και οι αναδυόμενοι κίνδυνοι από την κβαντική υπολογιστική, καθώς και τις αντίστοιχες ερευνητικές κατευθύνσεις που προτείνονται για την αντιμετώπισή τους.

6.2.1. Ευπάθειες σε Επίθεση 51% (51% Attack)

6.2.1.1 Ανάλυση Πρόκλησης

Ένας από τους πλέον διαδεδομένους και ταυτόχρονα επικίνδυνους περιορισμούς που συνδέονται με την ασφάλεια των δημόσιων blockchain δικτύων είναι η ευπάθεια σε επιθέσεις τύπου 51% (51% attack). Το συγκεκριμένο είδος κακόβουλης ενέργειας αφορά την περίπτωση κατά την οποία ένας ή περισσότεροι κόμβοι ελέγχουν συλλογικά πάνω από το 50% της συνολικής υπολογιστικής ισχύος του δικτύου (hashrate), γεγονός που τους παρέχει τη δυνατότητα να παρεμβαίνουν στη διαδικασία επικύρωσης συναλλαγών και στη διαμόρφωση των blocks [1]. Η ιδιαιτερότητα αυτού του φαινομένου έγκειται στο ότι θέτει υπό αμφισβήτηση τη βασική αρχή που διέπει

τις δημόσιες κατανεμημένες αλυσίδες, δηλαδή την ακεραιότητα και την εμπιστοσύνη που απορρέει από τη συναίνεση μεταξύ ανεξάρτητων συμμετεχόντων.

Όταν μία οντότητα καταφέρει να συγκεντρώσει τη συγκεκριμένη πλειοψηφία, αποκτά πρακτικά τον έλεγχο της δημιουργίας νέων blocks, επιτρέποντάς της να πραγματοποιήσει διπλές δαπάνες (double-spending)[15] ή ακόμα και να αποτρέψει την καταγραφή ορισμένων συναλλαγών στο καθολικό (ledger). Ειδικότερα, η δυνατότητα αναδιοργάνωσης της αλυσίδας (chain reorganization) δίνει στους επιτιθέμενους την ευχέρεια να διαγράφουν πρόσφατα blocks και να αναδιαμορφώνουν το ιστορικό συναλλαγών, υπονομεύοντας τη διαφάνεια και την αξιοπιστία του συστήματος [4]. Το πρόβλημα γίνεται οξύτερο σε περιβάλλοντα fog και edge computing, όπου οι υπολογιστικοί πόροι είναι περιορισμένοι, καθιστώντας τα δίκτυα ενδεχομένως πιο ευάλωτα σε συγκεντρωτικές επιθέσεις, δεδομένου ότι λιγότεροι συμμετέχοντες διαθέτουν ισχυρή υπολογιστική ισχύ.

Ακόμη, αξίζει να σημειωθεί ότι οι επιθέσεις 51% συνδέονται στενά με το κυρίαρχο μοντέλο συναίνεσης Proof of Work, το οποίο χρησιμοποιείται σε blockchains όπως το Bitcoin [1]. Το συγκεκριμένο μοντέλο βασίζεται στην επίλυση μαθηματικών προβλημάτων, διαδικασία που απαιτεί σημαντική υπολογιστική ισχύ. Ως αποτέλεσμα, οι συμμετέχοντες με μεγαλύτερη επεξεργαστική δυνατότητα αποκτούν συγκριτικό πλεονέκτημα, δημιουργώντας συνθήκες συγκέντρωσης ισχύος, γεγονός που αντιβαίνει στη θεμελιώδη αρχή της αποκέντρωσης.

Αξιοσημείωτη είναι επίσης η οικονομική διάσταση της επίθεσης. Η απόκτηση της απαιτούμενης ισχύος για την εκτέλεση μιας 51% attack σε μεγάλα δίκτυα, όπως το Bitcoin, προϋποθέτει τεράστιες επενδύσεις σε εξειδικευμένο υλικό (ASICs) και κατανάλωση ηλεκτρικής ενέργειας. Αντιθέτως, μικρότερα ή νεότερα blockchains, τα οποία ενδεχομένως να ενσωματωθούν σε fog και edge υποδομές, είναι συχνά πιο ευάλωτα, ιδίως στα αρχικά στάδια λειτουργίας τους, όταν ο αριθμός συμμετεχόντων (miners/validators) και η συνολική ισχύς ή το συνολικό stake παραμένουν περιορισμένα, με αποτέλεσμα το κόστος επίθεσης παραμένει αισθητά χαμηλότερο [5]. Έτσι, η εφαρμογή blockchains σε τέτοια κατανεμημένα περιβάλλοντα επιβάλλει τη διαρκή αξιολόγηση του κινδύνου συγκέντρωσης ισχύος, ώστε να διασφαλιστεί η αξιοπιστία των συναλλαγών και η εμπιστοσύνη στο σύστημα.

6.2.1.2 Ερευνητικές Κατευθύνσεις

Προκειμένου να αμβλυνθούν οι κίνδυνοι που απορρέουν από τις επιθέσεις 51%, έχουν προταθεί διάφορες ερευνητικές κατευθύνσεις, οι οποίες στοχεύουν είτε στη μείωση της πιθανότητας συγκέντρωσης υπολογιστικής ισχύος είτε στη

[15] *Double-spending* ονομάζεται η κακόβουλη πρακτική κατά την οποία ο ίδιος ψηφιακός πόρος/νόμισμα δαπανάται περισσότερες από μία φορές, μέσω δημιουργίας/διάδοσης αντικρουόμενων συναλλαγών. Σε blockchain συστήματα αυτό μπορεί να επιτευχθεί όταν ο επιτιθέμενος καταφέρει να αντιστρέψει ή να "αντικαταστήσει" πρόσφατα blocks (π.χ. μέσω αναδιοργάνωσης της αλυσίδας), ώστε να ακυρωθεί η αρχική συναλλαγή και να επικρατήσει εναλλακτικό ιστορικό όπου τα ίδια κεφάλαια εμφανίζονται ως διαθέσιμα.

διαμόρφωση υβριδικών μηχανισμών συναίνεσης που συνδυάζουν τα πλεονεκτήματα διαφορετικών αρχιτεκτονικών.

Multi-party Consensus / Validation. Μία από τις πιο αξιοσημείωτες προσεγγίσεις αφορά τη διερεύνηση πολυμερών (multi-party) μηχανισμών συναίνεσης, οι οποίοι απαιτούν τη συνεργασία διαφορετικών ομάδων συμμετεχόντων για την έγκριση blocks. Οι μηχανισμοί αυτοί μειώνουν τον κίνδυνο μονοπώλησης ισχύος από μία μόνο οντότητα, καθώς απαιτούν τη σύμπραξη διαφόρων ανεξάρτητων ομάδων για την επιτυχή καταχώρηση συναλλαγών [5].

Υβριδικά μοντέλα συναίνεσης PoW/PoS. Ιδιαίτερη έμφαση έχει δοθεί στην υιοθέτηση υβριδικών μοντέλων συναίνεσης, τα οποία συνδυάζουν το Proof of Work με το Proof of Stake. Ο όρος «υβριδικό» δεν σημαίνει ότι τα δύο μοντέλα λειτουργούν ταυτόχρονα με τον ίδιο τρόπο σε κάθε βήμα, αλλά ότι κατανέμονται διαφορετικοί ρόλοι μεταξύ τους. Συχνά, το PoW χρησιμοποιείται ως μηχανισμός παραγωγής blocks (block production) και αρχικής επιλογής/ανοχής σε Sybil, ενώ το PoS αξιοποιείται συμπληρωματικά για την οριστικοποίηση (finality) ή/και για τη διαδικασία επικύρωσης μέσω συμμετοχής κόμβων που δεσμεύουν stake. Εναλλακτικά, σε ορισμένες υλοποιήσεις το PoW παρέχει το “δικαίωμα” πρότασης block, αλλά η αποδοχή του block απαιτεί και επιβεβαίωση από PoS validators, ώστε να δυσκολεύεται ο επιτιθέμενος που βασίζεται αποκλειστικά σε υπολογιστική ισχύ. Το Proof of Stake βασίζεται στην κατοχή και διατήρηση συγκεκριμένου αριθμού tokens, μειώνοντας σημαντικά τις απαιτήσεις σε υπολογιστική ισχύ και, κατ’ επέκταση, περιορίζοντας τον κίνδυνο συγκέντρωσης ισχύος. Η συνδυαστική εφαρμογή των δύο προσεγγίσεων επιτρέπει τη διατήρηση του υψηλού επιπέδου ασφάλειας που παρέχει το Proof of Work, ενώ ταυτόχρονα ενισχύει την αποκέντρωση μέσω της συμμετοχής περισσότερων χρηστών, χωρίς να απαιτείται η απόκτηση ακριβού εξοπλισμού [4].

Hierarchical trust architecture (fog-specific). Παρότι τα υβριδικά μοντέλα PoW/PoS μειώνουν τον κίνδυνο συγκέντρωσης ισχύος μεταφέροντας μέρος της “ασφάλειας” από την υπολογιστική ισχύ στο οικονομικό stake, δεν αντιμετωπίζουν πλήρως τις ιδιαιτερότητες των fog/edge αρχιτεκτονικών, όπου η συμμετοχή είναι ετερογενής και συχνά πολυεπίπεδη. Για τον λόγο αυτό, παράλληλα με τις καθαρά κρυπτοοικονομικές λύσεις, προτείνονται και αρχιτεκτονικές προσεγγίσεις που αξιοποιούν τη δομή του fog/edge οικοσυστήματος για την ενίσχυση της εμπιστοσύνης και τον περιορισμό συγκεντρωτικών επιθέσεων. Μια επιπλέον κατεύθυνση, ειδικά σχετική με fog περιβάλλοντα, είναι η υιοθέτηση *ιεραρχικών αρχιτεκτονικών εμπιστοσύνης* (hierarchical trust), όπου η διαδικασία επικύρωσης και ο έλεγχος συνέπειας οργανώνονται πολυεπίπεδα. Σε τέτοια σχήματα, οι fog κόμβοι λειτουργούν ως ενδιάμεσοι “trust anchors” ή aggregators για ομάδες edge συσκευών, επιτρέποντας τοπική επικύρωση/φιλτράρισμα και στη συνέχεια περιοδική ενοποίηση σε ανώτερο επίπεδο. Με αυτόν τον τρόπο, μειώνεται η πιθανότητα μια μεμονωμένη οντότητα να επηρεάσει δυσανάλογα τη συνολική διαδικασία παραγωγής blocks, ενώ παράλληλα ενισχύεται η λειτουργική ανθεκτικότητα σε περιβάλλοντα με ετερογένεια και περιορισμένους πόρους.

Stake and role diversification. Παράλληλα, προτείνονται στρατηγικές *διαφοροποίησης stake και ρόλων* (stake/role diversification), όπου η συμμετοχή στη συναίνεση δεν εξαρτάται μονοδιάστατα από έναν παράγοντα (π.χ. μόνο hashrate ή μόνο stake), αλλά κατανέμεται σε διαφορετικούς ρόλους (proposers/validators/observers) και σε ομάδες κόμβων με διαφορετικά χαρακτηριστικά. Η διαφοροποίηση αυτή μειώνει τον κίνδυνο συγκέντρωσης ισχύος, καθώς ένας επιτιθέμενος θα έπρεπε να ελέγξει ταυτόχρονα πολλαπλές "διαστάσεις" συμμετοχής (υπολογιστική ισχύ, stake, ρόλους ή/και επίπεδα fog/edge) για να επιτύχει αντίστοιχη κυριαρχία.

Threshold & quorum-based validation. Σημαντική είναι και η κατεύθυνση *threshold/quorum-based validation*, όπου ένα block ή μια κρίσιμη ενέργεια θεωρείται έγκυρη μόνο όταν επιβεβαιωθεί από ένα κατώφλι (threshold) ή από ένα quorum ανεξάρτητων επικυρωτών. Σε αντίθεση με πιο "μονοκεντρικά" μοντέλα παραγωγής blocks, τα quorum σχήματα δυσκολεύουν την πρακτική εκμετάλλευση της πλειοψηφίας, επειδή απαιτούν ταυτόχρονη σύμπραξη/συνυπογραφή από πολλαπλές οντότητες, μειώνοντας την πιθανότητα αναδιοργάνωσης της αλυσίδας ή επιβολής censoring από έναν ισχυρό συμμετέχοντα.

Incentive misalignment (discouragement). Τέλος, μια πιο "οικονομική" γραμμή άμυνας αφορά τον σχεδιασμό μηχανισμών *αποθάρρυνσης μέσω κινήτρων* (incentive misalignment), ώστε η εκδήλωση επίθεσης 51% να καθίσταται μη συμφέρουσα. Αυτό μπορεί να επιτευχθεί με μηχανισμούς που αυξάνουν το αναμενόμενο κόστος της κακόβουλης συμπεριφοράς (π.χ. απώλεια ανταμοιβών, αποκλεισμός/penalties, ή οικονομική "έκθεση" μέσω stake σε υβριδικά σχήματα), καθιστώντας την επίθεση λιγότερο ελκυστική ακόμη και αν είναι τεχνικά εφικτή. Έτσι, ενισχύεται η ασφάλεια όχι μόνο τεχνικά αλλά και οικονομικά, ιδίως σε μικρότερα ή νεότερα δίκτυα όπου το "καθαρά τεχνικό" κόστος επίθεσης μπορεί να είναι χαμηλότερο [5].

Ανίχνευση ανωμαλιών ισχύος. Οι παραπάνω προσεγγίσεις στοχεύουν κυρίως στην πρόληψη της συγκέντρωσης ισχύος μέσω αρχιτεκτονικού σχεδιασμού, διαφοροποίησης ρόλων και οικονομικών αντικινήτρων. Ωστόσο, δεδομένου ότι καμία σχεδίαση δεν αποκλείει πλήρως το ενδεχόμενο σταδιακής συγκέντρωσης ισχύος στην πράξη, συμπληρωματικά απαιτούνται και μηχανισμοί έγκαιρης ανίχνευσης και απόκρισης, ώστε να αναγνωρίζονται ύποπτες αποκλίσεις πριν οδηγήσουν σε επιτυχημένη επίθεση. Στο πλαίσιο αυτό, ερευνητικό ενδιαφέρον συγκεντρώνει η ενσωμάτωση μηχανισμών ανίχνευσης ανωμαλιών και αποκεντρωμένων δικλίδων ασφαλείας, οι οποίοι επιτρέπουν την έγκαιρη αναγνώριση ύποπτων συγκεντρώσεων ισχύος. Τα συστήματα αυτά βασίζονται στη διαρκή παρακολούθηση της κατανομής του hashrate[16], ενώ ενεργοποιούν μηχανισμούς συναγερμού και αυτοματοποιημένες διαδικασίες επιβεβαίωσης, σε περιπτώσεις που διαπιστώνεται απόκλιση από τα φυσιολογικά πρότυπα λειτουργίας.

[16] Hashrate: ο ρυθμός εκτέλεσης υπολογισμών κατακερματισμού (hash functions) από έναν κόμβο ή από το σύνολο του δικτύου. Στα PoW blockchains χρησιμοποιείται ως ένδειξη της συνολικής υπολογιστικής ισχύος που συμμετέχει στην εξόρυξη και στην επικύρωση blocks.

Συνεπώς, η διατήρηση της ακεραιότητας και της αξιοπιστίας των δημόσιων blockchains, ιδιαίτερα όταν αυτά ενσωματώνονται σε περιβάλλοντα fog και edge computing, προϋποθέτει τη συνεχή ανάπτυξη και εφαρμογή καινοτόμων προσεγγίσεων που ενισχύουν την ανθεκτικότητα των συστημάτων σε επιθέσεις 51%. Οι ανωτέρω κατευθύνσεις δύνανται να συμβάλουν στη δημιουργία ασφαλέστερων και περισσότερο αποκεντρωμένων blockchain δικτύων, ικανών να ανταποκριθούν στις αυξημένες απαιτήσεις των σύγχρονων κατανεμημένων υποδομών.

6.2.2. Κενά σε έξυπνα συμβόλαια (smart contract vulnerabilities)

6.2.2.1 Ανάλυση Πρόκλησης

Τα έξυπνα συμβόλαια (smart contracts) αποτελούν μια καινοτόμο εφαρμογή της τεχνολογίας blockchain, παρέχοντας τη δυνατότητα αυτοματοποιημένης εκτέλεσης συμφωνιών μεταξύ συμβαλλομένων χωρίς τη μεσολάβηση τρίτου μέρους. Ωστόσο, παρά τη χρησιμότητά τους, έχουν αναδειχθεί ως σημαντική πηγή κινδύνων στον τομέα της ασφάλειας, γεγονός που καθιστά την ανάλυση των ευπαθειών τους απαραίτητη [4], [5].

Μια από τις βασικότερες αδυναμίες των έξυπνων συμβολαίων έγκειται στο γεγονός ότι, σε αντίθεση με το κλασικό λογισμικό, οι συναλλαγές που βασίζονται σε αυτά είναι μη αναστρέψιμες. Επομένως, οποιοδήποτε σφάλμα στον πηγαίο κώδικα μπορεί να αξιοποιηθεί από κακόβουλους χρήστες, οδηγώντας σε οικονομικές απώλειες. Το φαινόμενο αυτό κατέστη ιδιαιτέρως εμφανές σε περιστατικά όπως το συμβάν της πλατφόρμας DAO, το οποίο είχε ως αποτέλεσμα την απώλεια εκατομμυρίων δολαρίων λόγω κενών ασφαλείας στον κώδικα του έξυπνου συμβολαίου που χρησιμοποιήθηκε [4].

Ένα σημαντικό χαρακτηριστικό των συγκεκριμένων συμβολαίων είναι ότι αναπτύσσονται κυρίως σε γλώσσες προγραμματισμού όπως η Solidity. Παρότι οι γλώσσες αυτές είναι σχεδιασμένες ώστε να ανταποκρίνονται στις ιδιαιτερότητες των αποκεντρωμένων εφαρμογών, παρουσιάζουν πολυπλοκότητες που αυξάνουν τις πιθανότητες λανθασμένης υλοποίησης. Πιο συγκεκριμένα, έχει διαπιστωθεί πως ορισμένες λειτουργίες των έξυπνων συμβολαίων, όπως η αναδρομική κλήση (reentrancy), μπορούν να αξιοποιηθούν για τη δόλια απόσπαση κεφαλαίων από συμβόλαια, τα οποία δεν έχουν προβλεφθεί για τέτοιες περιπτώσεις [5].

Σε αυτό το σημείο, ένα ακόμη ζήτημα προκύπτει από το γεγονός ότι πολλές φορές οι προγραμματιστές δεν διαθέτουν την απαιτούμενη εξειδίκευση στον τομέα της ασφάλειας των έξυπνων συμβολαίων, με αποτέλεσμα να ενσωματώνουν πρακτικές ανάπτυξης που εφαρμόζονται σε συμβατικά πληροφοριακά συστήματα, αλλά δεν είναι επαρκείς για τα αποκεντρωμένα περιβάλλοντα. Το γεγονός αυτό ενισχύει τον κίνδυνο εκμετάλλευσης ατελειών στον κώδικα, καθώς η αρχιτεκτονική των blockchain συστημάτων απαιτεί αυξημένη ακρίβεια και ιδιαίτερη προσοχή στη διαχείριση των λογικών ροών [4].

Συνακόλουθα, οι ευπάθειες αυτές καθιστούν απαραίτητη την ενσωμάτωση στρατηγικών ενίσχυσης της ανθεκτικότητας των έξυπνων συμβολαίων ήδη από το στάδιο του σχεδιασμού τους. Προς αυτή την κατεύθυνση, έχουν προταθεί

διάφορες πρακτικές, όπως η αρχή του ελαχίστου προνομίου, η οποία προβλέπει ότι κάθε τμήμα του κώδικα πρέπει να διαθέτει μόνο τα απολύτως αναγκαία δικαιώματα για την εκτέλεση της συγκεκριμένης λειτουργίας. Επίσης, αναγνωρίζεται η ανάγκη για τη διενέργεια διαρκούς επιθεώρησης και ελέγχου των συμβολαίων, τόσο πριν από την ανάπτυξή τους στο δίκτυο, όσο και σε τακτική βάση κατά τη λειτουργία τους [5].

Καθώς οι αποκεντρωμένες εφαρμογές επεκτείνονται σε διάφορους τομείς, όπως τα οικονομικά, η εφοδιαστική αλυσίδα και η υγειονομική περίθαλψη, οι επιπτώσεις από πιθανές παραβιάσεις των έξυπνων συμβολαίων καθίστανται ολοένα και πιο σοβαρές. Συνεπώς, η θωράκισή τους αποτελεί προτεραιότητα για την ευρύτερη αποδοχή και αξιοποίηση της τεχνολογίας blockchain.

6.2.2.2 Ερευνητικές Κατευθύνσεις

Προκειμένου να περιοριστούν οι κίνδυνοι που απορρέουν από τις ευπάθειες των έξυπνων συμβολαίων, η επιστημονική κοινότητα έχει στραφεί προς την ανάπτυξη νέων εργαλείων και μεθοδολογιών που στοχεύουν στην ανίχνευση και αποτροπή λαθών ασφαλείας στον κώδικά τους.

Static & dynamic analysis tools. Μια από τις βασικές προτάσεις είναι η δημιουργία λογισμικών ανάλυσης στατικού και δυναμικού τύπου, τα οποία εξετάζουν τον πηγαίο κώδικα πριν από την ανάπτυξή του στο δίκτυο (του blockchain), με σκοπό να εντοπιστούν πιθανά κενά. Ειδικότερα, εργαλεία ανάλυσης όπως το Mythril[17] και το Oyente[18] έχουν εφαρμοστεί σε πλατφόρμες όπως το Ethereum, επιτρέποντας την έγκαιρη αναγνώριση επικίνδυνων προγραμματιστικών πρακτικών [5].

Secure standards & development guidelines. Πέρα από την ανίχνευση λαθών μέσω εργαλείων στατικής και δυναμικής ανάλυσης, σημαντικό ρόλο στη μείωση των ευπαθειών διαδραματίζει και η τυποποίηση της ανάπτυξης έξυπνων συμβολαίων μέσω ασφαλών προτύπων (standards) και κατευθυντήριων γραμμών προς τους προγραμματιστές. Η προσέγγιση αυτή προάγει τη διαλειτουργικότητα, ενισχύει την προβλεψιμότητα της συμπεριφοράς του κώδικα και συμβάλλει στη διαμόρφωση συμβολαίων που ακολουθούν βέλτιστες πρακτικές ασφαλείας. Για παράδειγμα, το πρότυπο ERC-20[19] έχει καθιερωθεί ως το πλέον διαδεδομένο για την ανάπτυξη διακριτικών (tokens)

[17] Εργαλείο ανάλυσης ασφάλειας για *smart contracts* στο Ethereum, που εκτελεί *symbolic execution* και τεχνικές ανίχνευσης ευπαθειών (π.χ. reentrancy, integer overflows/underflows, unchecked calls) σε bytecode/EVM επίπεδο, με στόχο τον εντοπισμό σφαλμάτων πριν την ανάπτυξη του συμβολαίου.

[18] Πρωτοπόρο ερευνητικό εργαλείο στατικής ανάλυσης για Ethereum *smart contracts*, βασισμένο σε *symbolic execution*, το οποίο στοχεύει στον εντοπισμό τυπικών ευπαθειών (π.χ. reentrancy, timestamp dependence, transaction-ordering dependence) μέσω ανάλυσης της EVM εκτέλεσης.

[19] Πρότυπο (standard) διασύνδεσης για *fungible tokens* στο Ethereum, που ορίζει ένα σύνολο βασικών συναρτήσεων και events (π.χ. transfer, approve, transferFrom, allowance) ώστε τα tokens να είναι διαλειτουργικά με πορτοφόλια, ανταλλακτήρια και εφαρμογές.

στο Ethereum, ωστόσο έχουν αναδειχθεί βελτιωμένες εκδοχές, όπως το ERC-777[20], που παρέχουν πρόσθετους μηχανισμούς ασφαλείας [4].

Formal methods (formal specification & verification). Μία ακόμη ισχυρή κατεύθυνση είναι η εφαρμογή *formal methods (τυπικών μεθόδων)*, όπου το συμβόλαιο συνοδεύεται από τυπική προδιαγραφή (formal specification) και ελέγχεται με μεθόδους επαλήθευσης (formal verification) ότι ικανοποιεί συγκεκριμένες ιδιότητες ασφάλειας (π.χ. “δεν μπορεί να μειωθεί αυθαίρετα το υπόλοιπο”, “δεν παρακάμπτονται δικαιώματα”, “δεν δημιουργούνται μη αναμενόμενες καταστάσεις”). Η προσέγγιση αυτή είναι ιδιαίτερα χρήσιμη σε κρίσιμα συμβόλαια (π.χ. tokens, vaults, governance), όπου ένα σφάλμα μπορεί να έχει μη αναστρέψιμες οικονομικές συνέπειες.

Security-by-design, minimalism & attack-surface reduction. Ωστόσο, η ύπαρξη προτύπων και εργαλείων ελέγχου δεν αρκεί από μόνη της για την εξάλειψη κρίσιμων σφαλμάτων, καθώς πολλές ευπάθειες προκύπτουν από λογικές αστοχίες, λανθασμένες παραδοχές εμπιστοσύνης ή επικίνδυνες επιλογές αρχιτεκτονικής. Για τον λόγο αυτό, σημαντική κατεύθυνση αποτελεί η υιοθέτηση αρχών security-by-design ήδη από το στάδιο του σχεδιασμού. Κεντρική πρακτική είναι η ελαχιστοποίηση της πολυπλοκότητας και των «εκτεθειμένων» σημείων ενός συμβολαίου, όπως λιγότερες λειτουργίες, απλούστερες ροές και περιορισμός δικαιωμάτων, ώστε να μειώνεται το περιθώριο λαθών και να καθίσταται δυσκολότερη η εκμετάλλευση ευπαθειών. Παράλληλα, προτείνεται η σαφής αποτύπωση explicit trust assumptions, δηλαδή του ποιον εμπιστευόμαστε και υπό ποιες προϋποθέσεις, ώστε ο σχεδιασμός να μην βασίζεται σε άτυπες ή σιωπηρές παραδοχές.

Safe language & compiler choices. Επιπλέον, προτείνεται η χρήση ασφαλέστερων επιλογών σε επίπεδο γλώσσας και μεταγλωττιστή (*safe language & compiler choices*), όπως η υιοθέτηση πιο “περιοριστικών”/ασφαλών υποσυνόλων γλώσσας, αυστηρών ρυθμίσεων compiler, καθώς και εργαλείων που αποτρέπουν επικίνδυνα μοτίβα (π.χ. μη ελεγχόμενες κλήσεις, ανεπαρκείς έλεγχοι ορίων/καταστάσεων). Στόχος είναι να μειωθεί ο κίνδυνος λογικών σφαλμάτων και να ενισχυθεί η προβλεψιμότητα της εκτέλεσης στο EVM περιβάλλον.

Secure design patterns. Σε επίπεδο πρακτικών υλοποίησης, ιδιαίτερη βαρύτητα έχει η εφαρμογή *secure design patterns*. Ενδεικτικά, το μοτίβο *Checks-Effects-Interactions* προτείνει να γίνονται πρώτα όλοι οι έλεγχοι, έπειτα οι αλλαγές κατάστασης και τέλος οι εξωτερικές κλήσεις, ώστε να μετριάζεται ο κίνδυνος re-entrancy[21]. Παράλληλα, η αρχή *pull over push payments* (δηλ. ο χρήστης “τραβά” τα χρήματα αντί το συμβόλαιο να τα “σπρώχνει” αυτόματα) μειώνει την έκθεση σε αποτυχημένες εξωτερικές κλήσεις και DoS καταστάσεις. Αντίστοιχα,

---

[20] Πρότυπο για *fungible tokens* στο Ethereum που επεκτείνει/βελτιώνει το ERC-20, εισάγοντας μηχανισμούς *hooks* (callbacks) μέσω του προτύπου ERC-1820, επιτρέποντας σε συμβόλαια/λήπτες να αντιδρούν σε μεταφορές tokens και υποστηρίζοντας πιο εκφραστικές λειτουργίες· παραμένει συμβατό προς τα πίσω με ERC-20 σε πολλά σενάρια.

[21] **Re-entrancy**: ευπάθεια κατά την οποία ένα έξυπνο συμβόλαιο δέχεται νέα κλήση προς κρίσιμη συνάρτησή του πριν ολοκληρωθεί η προηγούμενη εκτέλεση και πριν ενημερωθεί ορθά η εσωτερική του κατάσταση. Αυτό μπορεί να επιτρέψει σε κακόβουλο συμβόλαιο να επαναλάβει την ίδια ενέργεια πολλές φορές, οδηγώντας, για παράδειγμα, σε μη εξουσιοδοτημένη ανάληψη ή μεταφορά κεφαλαίων.

προτείνεται το μοτίβο *guarded access control* με σαφείς ρόλους/δικαιώματα και αυστηρή επιβολή τους, που μειώνει τον κίνδυνο κατάχρησης προνομίων.

External dependency hardening. Επιπλέον, δίνεται έμφαση στη θωράκιση εξωτερικών εξαρτήσεων (*external dependency hardening*), όπως βιβλιοθήκες τρίτων, oracles, ή άλλα συμβόλαια με τα οποία γίνεται αλληλεπίδραση. Καθώς η ασφάλεια ενός συμβολαίου μπορεί να υπονομευθεί από ένα ευάλωτο dependency, προτείνονται έλεγχοι εκδόσεων, περιορισμός αλληλεπιδράσεων, και σαφείς πολιτικές fallback σε περιπτώσεις σφαλμάτων/ασυνέπειας.

Beyond conventional testing (property-based & adversarial testing). Πέρα από τα συμβατικά tests, προτείνεται η χρήση *property-based testing* (έλεγχος ιδιοτήτων που πρέπει να ισχύουν για πολλές τυχαίες εισόδους/σενάρια) και *adversarial testing* (δοκιμές με “εχθρικά” μοτίβα εισόδων), ώστε να εντοπίζονται edge-cases που δεν καλύπτονται εύκολα με χειροκίνητα σενάρια. Με αυτό τον τρόπο αυξάνεται η πιθανότητα να ανιχνευθούν λογικά σφάλματα πριν τη μη αναστρέψιμη ανάπτυξη στο δίκτυο.

Runtime protection mechanisms. Πέρα από τον σχεδιασμό, συναντώνται μηχανισμοί προστασίας κατά τον χρόνο εκτέλεσης (*runtime protection mechanisms*). Ενδεικτικά, *reentrancy guards* αποτρέπουν επαναληπτικές εισόδους σε κρίσιμες συναρτήσεις, ενώ τεχνικές όπως *rate limiting & circuit breakers* μπορούν να “φρενάρουν” ύποπτη δραστηριότητα ή να θέτουν προσωρινά το συμβόλαιο σε ασφαλή κατάσταση (pause) όταν ανιχνευθούν ανωμαλίες. Επιπλέον, ο μηχανισμός *gas-aware logic* βοηθά στη μείωση κινδύνων που σχετίζονται με εξάντληση gas ή επιθέσεις που εκμεταλλεύονται το κόστος εκτέλεσης (π.χ. λειτουργίες που γίνονται απρόβλεπτα ακριβές).

Upgradeable-contract safety. Επειδή πολλά συμβόλαια εξελίσσονται, ιδιαίτερο ζήτημα αποτελεί η ασφάλεια των αναβαθμίσεων (*upgradeable-contract safety*). Προτείνεται η *controlled upgradeability* (σαφείς και περιορισμένοι ρόλοι αναβάθμισης, χρονικές καθυστερήσεις/timelocks, πολλαπλές υπογραφές) και, όπου είναι δυνατό, η ύπαρξη *immutable core logic* (αμετάβλητος πυρήνας κρίσιμων κανόνων), ώστε η αναβάθμιση να μην μετατρέπεται σε “κρυφή πίσω πόρτα” ή σε σημείο κατάχρησης εξουσίας.

Runtime monitoring & on-chain defense. Τέλος, ολοένα και περισσότερο συζητούνται λύσεις *runtime monitoring & on-chain defense*, όπου παρακολουθούνται κρίσιμες μεταβλητές/συμπεριφορές μετά την ανάπτυξη (π.χ. ασυνήθιστες ροές κεφαλαίων, απότομες μεταβολές κατάστασης), και ενεργοποιούνται μηχανισμοί άμυνας (alerts, pause, περιορισμοί) ώστε να περιορίζεται η ζημιά σε περίπτωση πραγματικής εκμετάλλευσης.

Συνολικά, οι παραπάνω προσεγγίσεις δείχνουν ότι η ασφάλεια των έξυπνων συμβολαίων δεν εξαρτάται από ένα μόνο μέτρο, αλλά απαιτεί πολυεπίπεδη στρατηγική που εκκινεί από τον σχεδιασμό και φτάνει έως τη λειτουργική παρακολούθηση μετά την ανάπτυξη.

Στο πλαίσιο αυτό, καθίσταται σαφές ότι η ενίσχυση της ασφάλειας των έξυπνων συμβολαίων απαιτεί συνδυαστική προσέγγιση, η οποία περιλαμβάνει τόσο την τεχνολογική υποστήριξη μέσω λογισμικών ανάλυσης, όσο και την εδραίωση

κοινά αποδεκτών κανόνων και διαδικασιών που θα διέπουν την ανάπτυξη και τον έλεγχο των εφαρμογών blockchain.

6.2.3. Ζητήματα Ιδιωτικότητας Συναλλαγών

6.2.3.1 Ανάλυση Πρόκλησης

Η προστασία της ιδιωτικότητας των συναλλαγών στο πλαίσιο των κατανεμημένων λογιστικών βιβλίων αποτελεί θεμελιώδη πρόκληση, καθώς οι αλυσίδες blockchain, ειδικά όταν πρόκειται για δημόσια δίκτυα, χαρακτηρίζονται από εγγενή διαφάνεια. Όλες οι συναλλαγές είναι ορατές και επαληθεύσιμες από οποιονδήποτε συμμετέχοντα, γεγονός που, ενώ ενισχύει τη διαφάνεια και την εμπιστοσύνη, ταυτόχρονα καθιστά δυσχερή τη διατήρηση της ανωνυμίας των χρηστών [9].

Η συγκεκριμένη ιδιαιτερότητα έχει οδηγήσει σε προβληματισμούς αναφορικά με τη διαχείριση ευαίσθητων πληροφοριών σε πλατφόρμες που εφαρμόζονται σε τομείς, όπως οι χρηματοοικονομικές υπηρεσίες, η υγειονομική περίθαλψη και οι εφοδιαστικές αλυσίδες. Ιδίως σε περιβάλλοντα που περιλαμβάνουν προσωπικά δεδομένα, η πλήρης αποκάλυψη των λεπτομερειών μιας συναλλαγής ενδέχεται να αντίκειται στις διατάξεις κανονιστικών πλαισίων όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR), γεγονός που καθιστά απαραίτητη την ανεύρεση ισορροπίας ανάμεσα στη διαφάνεια και τη διασφάλιση της ιδιωτικότητας [11].

Πέραν των προσωπικών δεδομένων, ζήτημα εγείρεται και ως προς τις επιχειρηματικές συναλλαγές, όπου η γνωστοποίηση στοιχείων όπως το ύψος των πληρωμών, των τιμών, οι χρόνοι εκτέλεσης ή ακόμη και τα εμπλεκόμενα μέρη, ενδέχεται να αποκαλύψει κρίσιμες πληροφορίες για την εμπορική στρατηγική μιας επιχείρησης. Σε τέτοιες περιπτώσεις, η αδιάλειπτη προσβασιμότητα στις πληροφορίες του blockchain μπορεί να οδηγήσει σε φαινόμενα βιομηχανικής κατασκοπείας ή να διευκολύνει τη χειραγώγηση της αγοράς και της διαπραγματευτικής θέσης της επιχείρησης, καθώς ανταγωνιστές ή συνεργάτες μπορούν να προσαρμόσουν τη δική τους στρατηγική με βάση τις αποκαλυπτόμενες πληροφορίες [5].

Ειδικά τα δημόσια δίκτυα, όπως το Bitcoin, βασίζονται σε ψευδώνυμα (pseudonymity), τα οποία αν και αρχικά θεωρήθηκαν επαρκή για την ανωνυμία των συναλλαγών, εντούτοις αποδείχθηκαν ευάλωτα. Μέσω τεχνικών ανάλυσης δικτύων συναλλαγών (transaction graph analysis), κακόβουλοι παράγοντες έχουν καταφέρει να συνδέσουν διευθύνσεις ψηφιακών πορτοφολιών με πραγματικές ταυτότητες χρηστών [9]. Αντιθέτως, τα ιδιωτικά και τα κοινοπρακτικά blockchains (consortium blockchains) προσφέρουν υψηλότερο επίπεδο ελέγχου, ωστόσο ακόμη και σε αυτά, η πρόσβαση στις συναλλαγές από συγκεκριμένους εμπλεκόμενους φορείς μπορεί να εκθέσει εμπιστευτικές πληροφορίες [5].

Από τη σκοπιά των επιχειρηματικών εφαρμογών, ο τομέας της φαρμακευτικής εφοδιαστικής αλυσίδας αποτελεί χαρακτηριστικό παράδειγμα όπου απαιτείται αυξημένη προστασία της ιδιωτικότητας. Οι οργανισμοί που συμμετέχουν στη διακίνηση φαρμάκων επιθυμούν μεν τη διαφάνεια για την αποτροπή πλαστών

προϊόντων, αλλά ταυτόχρονα αποβλέπουν στη διαφύλαξη κρίσιμων δεδομένων, όπως οι ποσότητες και οι εμπορικές συμφωνίες, από μη εξουσιοδοτημένα μέρη [11].

6.2.3.2 Ερευνητικές Κατευθύνσεις

Η επίλυση των ανωτέρω ζητημάτων έχει οδηγήσει στην ανάπτυξη εξειδικευμένων κρυπτογραφικών τεχνικών, οι οποίες αποσκοπούν στην ενίσχυση της ανωνυμίας και της εμπιστευτικότητας των συναλλαγών χωρίς να διακυβεύεται η ακεραιότητα του blockchain.

Zero-knowledge foundations (Zerocoin και zk-SNARKs). Σημαντικό βήμα προς αυτή την κατεύθυνση αποτέλεσε η εισαγωγή πρωτοκόλλων όπως το Zerocoin[22] και οι μη διαδραστικές αποδείξεις μηδενικής γνώσης (zk-SNARKs). Οι μέθοδοι αυτές επιτρέπουν την επικύρωση μιας συναλλαγής χωρίς την αποκάλυψη των εμπλεκόμενων στοιχείων, ενισχύοντας την προστασία της ιδιωτικότητας [5].

Παρότι οι αποδείξεις μηδενικής γνώσης αποτελούν κεντρικό άξονα της privacy-preserving κρυπτογραφίας, η βιβλιογραφία έχει προτείνει ένα ευρύτερο σύνολο τεχνικών, οι οποίες καλύπτουν διαφορετικά επίπεδα του οικοσυστήματος (πρωτόκολλο συναλλαγών, δικτυακό επίπεδο, επίπεδο διευθύνσεων, και επίπεδο εφαρμογής), ανάλογα με το είδος απειλής και τις απαιτήσεις συμμόρφωσης.

Προχωρημένες αποδείξεις μηδενικής γνώσης (zk-STARKs, bulletproofs). Πέρα από τα zk-SNARKs, έχουν προταθεί και άλλες τεχνολογίες μηδενικής γνώσης, όπως τα *zk-STARKs*, τα οποία στοχεύουν στη μείωση ή εξάλειψη της ανάγκης για “trusted setup[23]” σε ορισμένα σενάρια, καθώς και τα *bulletproofs*, που χρησιμοποιούνται κυρίως για συμπαγείς αποδείξεις σε δεσμεύσεις τιμών (range proofs). Οι προσεγγίσεις αυτές επιτρέπουν την επαλήθευση ιδιοτήτων μιας συναλλαγής (π.χ. εγκυρότητα, όρια τιμών) χωρίς αποκάλυψη των υποκείμενων δεδομένων, ενισχύοντας την εμπιστευτικότητα χωρίς να θίγεται η επαληθευσιμότητα.

zk-Rollups (privacy-preserving variants). Συμπληρωματικά, ερευνητική και πρακτική εξέλιξη παρουσιάζουν τα *zk-Rollups*, όπου πολλές συναλλαγές “συμπιέζονται” και επαληθεύονται συλλογικά μέσω μιας κρυπτογραφικής απόδειξης. Σε παραλλαγές που διατηρούν την ιδιωτικότητα (privacy-preserving variants), τα rollups μπορούν να επιτυγχάνουν όχι μόνο κλιμάκωση, αλλά και απόκρυψη κρίσιμων στοιχείων της συναλλαγής από το κύριο καθολικό, διατηρώντας ωστόσο την τελική επαληθευσιμότητα της ορθότητας.

---

[22] Πρωτόκολλο/κρυπτογραφικό σχήμα ενίσχυσης ιδιωτικότητας για κρυπτονομίσματα, το οποίο εισάγει μηχανισμό *μηδενικής γνώσης* (zero-knowledge proofs) ώστε ένας χρήστης να μπορεί να αποδείξει ότι κατέχει έγκυρο νόμισμα και να το “εξαργυρώσει” χωρίς να συνδέεται δημόσια η συναλλαγή εξαργύρωσης με την αρχική συναλλαγή δημιουργίας/κατάθεσης, προσφέροντας ισχυρότερη ανωνυμία σε σχέση με την απλή ψευδωνυμοποίηση των κλασικών blockchain [28].

[23] *Trusted setup*: προκαταρκτική διαδικασία αρχικοποίησης ορισμένων σχημάτων αποδείξεων μηδενικής γνώσης, κατά την οποία παράγονται δημόσιες παράμετροι που θα χρησιμοποιηθούν αργότερα στις αποδείξεις και την επαλήθευσή τους. Η διαδικασία αυτή θεωρείται ευαίσθητη, επειδή αν παραβιαστεί ή αν ο φορέας που τη διενεργεί δεν είναι αξιόπιστος, ενδέχεται να υπονομευθεί η ασφάλεια του σχήματος.

Παρότι οι ZK τεχνικές παρέχουν ισχυρές εγγυήσεις, δεν αποτελούν τη μοναδική προσέγγιση. Σε αρκετά περιβάλλοντα εφαρμόζονται τεχνικές *ανάμειξης* και *απόκρυψης* που στοχεύουν στη δυσκολία συσχέτισης εισερχόμενων και εξερχόμενων συναλλαγών, λειτουργώντας είτε ως συμπληρωματική άμυνα είτε ως πιο "ελαφριά" επιλογή όπου οι ZK αποδείξεις είναι δύσκολο να υλοποιηθούν.

Mixing & obfuscation techniques (CoinJoin/CoinShuffle, mixnets, tumblers). Τεχνικές όπως *CoinJoin* και *CoinShuffle* επιδιώκουν να συνδυάσουν συναλλαγές πολλών χρηστών σε κοινές δομές, ώστε να καθίσταται δυσκολότερη η αντιστοίχιση "ποιος πλήρωσε ποιον". Σε πιο γενικευμένο επίπεδο, *mixnets* και υπηρεσίες *tumblers/mixers* μπορούν να λειτουργήσουν ως ενδιάμεσοι μηχανισμοί απόκρυψης της προέλευσης/προορισμού, αυξάνοντας την αβεβαιότητα σε επιθέσεις ανάλυσης γραφήματος συναλλαγών. Παρότι οι τεχνικές αυτές ενισχύουν την ιδιωτικότητα, συχνά συνοδεύονται από trade-offs σε εμπιστοσύνη, καθυστέρηση και ρυθμιστικές απαιτήσεις, ειδικά όταν βασίζονται σε εξωτερικούς μεσολαβητές [4] [5].

Ring-based anonymity. Άλλη κατηγορία προσεγγίσεων είναι οι μηχανισμοί ανωνυμίας με βάση "δακτυλίους" (ring-based), όπου μια υπογραφή ή μια δαπάνη παρουσιάζεται ως προερχόμενη από ένα σύνολο πιθανών μελών. Έτσι, ο παρατηρητής δυσκολεύεται να ταυτοποιήσει ποιο μέλος του συνόλου πραγματοποίησε τη συναλλαγή, περιορίζοντας αποτελεσματικά την αντιστοίχιση διευθύνσεων σε πραγματικές οντότητες.

Εκτός από την απόκρυψη της ταυτότητας/συσχέτισης των διευθύνσεων, εξίσου κρίσιμη είναι σε επιχειρηματικά σενάρια η απόκρυψη του *ποσού* και άλλων εμπορικά ευαίσθητων χαρακτηριστικών μιας συναλλαγής.

Confidential Transactions (CT). Οι *Confidential Transactions* στοχεύουν στην απόκρυψη των ποσών διατηρώντας, ταυτόχρονα, την επαληθευσιμότητα ότι δεν δημιουργείται χρήμα "από το πουθενά". Αυτό επιτυγχάνεται μέσω κρυπτογραφικών δεσμεύσεων (π.χ. *Pedersen commitments* και γενικότερα *homomorphic commitments*), όπου το ποσό παραμένει κρυφό αλλά επιτρέπονται έλεγχοι συνέπειας (π.χ. ότι οι είσοδοι/έξοδοι "ισοσκελίζονται"). Έτσι, μειώνεται ο κίνδυνος αποκάλυψης εμπορικών πληροφοριών (τιμές, όγκοι συναλλαγών) σε δημόσια ή κοινοπρακτικά δίκτυα.

Address-level & network-layer privacy. Συμπληρωματικά, η ιδιωτικότητα μπορεί να ενισχυθεί σε επίπεδο διευθύνσεων (π.χ. συχνή εναλλαγή διευθύνσεων, αποφυγή επαναχρησιμοποίησης, "stealth" τεχνικές όπου είναι διαθέσιμες) και σε επίπεδο δικτύου, όπου στοχεύεται η μείωση διαρροών μεταδεδομένων μετάδοσης. Το τελευταίο είναι σημαντικό διότι, ακόμη και όταν το περιεχόμενο μιας συναλλαγής είναι κρυπτογραφημένο, μεταδεδομένα όπως χρονισμοί και μοτίβα διάδοσης μπορούν να βοηθήσουν σε συσχετισμούς χρηστών/κόμβων.

Τέλος, πέρα από καθαρά κρυπτογραφικές τεχνικές, η έρευνα εξετάζει και "υπολογιστικές" λύσεις ιδιωτικότητας, όπου κρίσιμες λειτουργίες εκτελούνται είτε σε προστατευμένα περιβάλλοντα εκτέλεσης είτε μέσω κατανεμημένων υπολογισμών που δεν αποκαλύπτουν τις εισόδους.

Trusted Execution Environments (TEE). Τα *TEE* επιτρέπουν την εκτέλεση κώδικα και επεξεργασία δεδομένων σε απομονωμένο περιβάλλον (enclave), μειώνοντας την ανάγκη αποκάλυψης ευαίσθητων πληροφοριών στους υπόλοιπους κόμβους. Σε fog/edge σενάρια, αυτό μπορεί να είναι ελκυστικό για ιδιωτικές ή κοινοπρακτικές εφαρμογές, αν και απαιτεί προσεκτική αξιολόγηση του μοντέλου εμπιστοσύνης και των κινδύνων υλοποίησης/side-channels.

Secure Multi-Party Computation (MPC/SMPC). Ο *ασφαλής πολυμερής υπολογισμός* επιτρέπει σε πολλούς συμμετέχοντες να υπολογίσουν ένα αποτέλεσμα συλλογικά χωρίς να αποκαλύψουν ο καθένας τα ιδιωτικά δεδομένα εισόδου. Σε περιβάλλοντα με πολλαπλούς φορείς (π.χ. consortium), η MPC μπορεί να λειτουργήσει ως μηχανισμός privacy-preserving επικύρωσης / επεξεργασίας, μειώνοντας την έκθεση δεδομένων μεταξύ οργανισμών.

Application-layer encryption. Τέλος, σε εφαρμογές όπου απαιτείται αυστηρός έλεγχος ορατότητας, μπορεί να εφαρμοστεί κρυπτογράφηση σε επίπεδο εφαρμογής, όπου τα δεδομένα παραμένουν κρυπτογραφημένα end-to-end και στο blockchain καταγράφονται μόνο όσα είναι αναγκαία για ακεραιότητα/ιχνηλασιμότητα (π.χ. hashes, pointers). Έτσι, επιτυγχάνεται πρακτική συμμόρφωση και προστασία εμπορικά/προσωπικά ευαίσθητων πληροφοριών, ενώ διατηρείται η δυνατότητα ελέγχου ακεραιότητας.

Selective disclosure. Εν παραλλήλω, εξετάζεται η εφαρμογή μηχανισμών επιλεκτικής αποκάλυψης δεδομένων (selective disclosure). Στο πλαίσιο αυτής της τεχνικής, ο χρήστης διατηρεί τον έλεγχο των πληροφοριών του, αποφασίζοντας ο ίδιος ποια στοιχεία θα καταστήσει ορατά σε τρίτους, εξυπηρετώντας ταυτόχρονα τις ανάγκες διαφάνειας και διαφύλαξης της εμπιστευτικότητας [9].

Hybrid privacy-preserving architectures. Εξίσου σημαντική, έχει αναδειχθεί η σημασία της υιοθέτησης υβριδικών προσεγγίσεων, στις οποίες συνδυάζονται δημόσια blockchains για τη διασφάλιση της διαφάνειας και ιδιωτικά υποσυστήματα για τη διαχείριση ευαίσθητων πληροφοριών. Οι συνδυαστικές αυτές πρακτικές αξιοποιούνται ήδη σε κλάδους όπως η υγειονομική περίθαλψη, όπου απαιτείται ταυτόχρονα διαφάνεια στην παρακολούθηση της πορείας των φαρμακευτικών προϊόντων και απόλυτη μυστικότητα στη διαχείριση των ιατρικών δεδομένων των ασθενών [11].

Η εξέλιξη της τεχνολογίας blockchain προς την κατεύθυνση της προστασίας της ιδιωτικότητας αποτελεί ένα από τα πιο ενεργά πεδία έρευνας, καθώς η επίτευξη της επιθυμητής ισορροπίας μεταξύ διαφάνειας και ανωνυμίας θεωρείται κομβικής σημασίας για την ευρεία αποδοχή και εφαρμογή των αποκεντρωμένων συστημάτων.

6.2.4. Κίνδυνοι από Κβαντικούς Υπολογιστές

6.2.4.1 Ανάλυση Πρόκλησης

Η αδιάκοπη εξέλιξη της πληροφορικής τεχνολογίας έχει αναδείξει τους κβαντικούς υπολογιστές ως μία από τις πλέον καινοτόμες και ενδεχομένως ανατρεπτικές επιστημονικές κατακτήσεις. Αν και η πλήρης αξιοποίησή τους

βρίσκεται ακόμη σε ερευνητικό στάδιο, η μελλοντική τους ανάπτυξη εγείρει ανησυχίες αναφορικά με τη θωράκιση της ασφάλειας στα κατανεμημένα λογιστικά βιβλία (blockchains), καθώς και στα ευρύτερα πληροφοριακά συστήματα που βασίζονται σε ασύμμετρη κρυπτογραφία [5].

Οι κβαντικοί υπολογιστές, σε αντίθεση με τα κλασικά συστήματα, αξιοποιούν την αρχή της υπέρθεσης (superposition) και της διεμπλοκής (entanglement), γεγονός που τους επιτρέπει να εκτελούν παράλληλους υπολογισμούς με εκθετικά ταχύτερους ρυθμούς. Αυτό σημαίνει ότι ένας ισχυρός κβαντικός υπολογιστής θα μπορούσε, δυνητικά, να επιλύσει προβλήματα που σήμερα θεωρούνται υπολογιστικά αδύνατο να επιλυθούν σε πρακτικούς χρόνους. Ενδεικτικά, ο αλγόριθμος Shor είναι ικανός να διασπάσει την παραδοσιακή κρυπτογραφία δημόσιου κλειδιού (public-key cryptography), όπως τα συστήματα RSA και ECDSA, που αποτελούν τη βάση ασφαλείας των περισσότερων υπαρχόντων blockchain πλατφορμών [4].

Αυτό το ενδεχόμενο έχει προκαλέσει έντονες συζητήσεις στη διεθνή επιστημονική κοινότητα, δεδομένου ότι η αποκάλυψη ενός ιδιωτικού κλειδιού από έναν κακόβουλο παράγοντα θα μπορούσε να επιτρέψει την πλαστογράφηση συναλλαγών, την παραποίηση ιστορικών δεδομένων ή ακόμη και τη μαζική υποκλοπή πορτοφολιών χρηστών. Μία τέτοια εξέλιξη θα έθετε υπό αμφισβήτηση τη βασική αρχή της ακεραιότητας και της εμπιστοσύνης, που διέπει την αρχιτεκτονική των blockchain δικτύων [5].

Ακόμη κι αν η απειλή αυτή φαντάζει μακρινή, οι ειδικοί επισημαίνουν ότι η χρονική συγκυρία ανάπτυξης των κβαντικών υπολογιστών ενδέχεται να συμπέσει με την ωρίμανση και ευρεία διάδοση των αποκεντρωμένων τεχνολογιών. Το λεγόμενο “Harvest Now, Decrypt Later” σενάριο έχει ήδη διατυπωθεί, υποδηλώνοντας πως ορισμένοι κακόβουλοι φορείς μπορεί σήμερα να συλλέγουν κρυπτογραφημένες πληροφορίες με σκοπό να τις αποκρυπτογραφήσουν όταν οι κβαντικές δυνατότητες το επιτρέψουν [5].

Η προσαρμογή των blockchains στη νέα πραγματικότητα της κβαντικής υπολογιστικής συνιστά, κατά συνέπεια, ζήτημα ζωτικής σημασίας. Οι φορείς ανάπτυξης των κατανεμημένων συστημάτων βρίσκονται ενώπιον μιας διττής πρόκλησης: αφενός, να διασφαλίσουν τη συνέχιση της απρόσκοπτης λειτουργίας των ήδη υπαρχόντων αλυσίδων, και αφετέρου, να θωρακίσουν τις μελλοντικές εφαρμογές τους έναντι των αναδυόμενων κινδύνων.

6.2.4.2 Ερευνητικές Κατευθύνσεις

Η επιστημονική κοινότητα, αναγνωρίζοντας τον επερχόμενο κίνδυνο, έχει ήδη στραφεί προς την ανάπτυξη μεθόδων κρυπτογράφησης ανθεκτικών στους κβαντικούς υπολογιστές, οι οποίες συλλογικά αναφέρονται ως Post-Quantum Cryptography (PQC).

Post-Quantum Cryptography (PQC). Η βασικότερη ερευνητική κατεύθυνση αφορά την ανάπτυξη κρυπτογραφικών τεχνικών που παραμένουν ασφαλείς ακόμη και απέναντι σε ισχυρούς κβαντικούς αντιπάλους. Οι τεχνικές αυτές βασίζονται σε μαθηματικά προβλήματα, όπως τα lattices (πλέγματα), οι αλγεβρικές εξισώσεις πάνω σε σώματα και οι πολυμεταβλητές πολυωνυμικές

συναρτήσεις, τα οποία δεν φαίνεται να επιλύονται αποτελεσματικά με χρήση των γνωστών κβαντικών αλγορίθμων [5].

Lattice-based cryptography & hash-based signatures. Μεταξύ των πλέον ελπιδοφόρων μεθόδων συγκαταλέγονται η lattice-based cryptography και οι hash-based υπογραφές. Η πρώτη κατηγορία, βασισμένη στη δυσκολία επίλυσης προβλημάτων πλέγματος, έχει καταγράψει ιδιαίτερη πρόοδο λόγω της ανθεκτικότητάς της απέναντι στις γνωστές κβαντικές επιθέσεις. Η δεύτερη κατηγορία, που αξιοποιεί αλγορίθμους όπως οι Lamport και Winternitz, διασφαλίζει την ακεραιότητα των ψηφιακών υπογραφών μέσω μη αναστρέψιμων συναρτήσεων κατακερματισμού, χωρίς να βασίζεται σε θεωρίες παραγοντοποίησης ή διακριτού λογαρίθμου, που πλήττονται άμεσα από τον αλγόριθμο Shor [4].

Υβριδικά και μεταβατικά σχήματα (hybrid / transitional schemes). Εξίσου κρίσιμη θεωρείται η ανάπτυξη μεταβατικών στρατηγικών, μέσω των οποίων τα παραδοσιακά κρυπτογραφικά σχήματα συνυπάρχουν με post-quantum τεχνικές. Η προσέγγιση αυτή επιτρέπει σταδιακή μετάβαση προς κβαντοανθεκτικές υποδομές, χωρίς να διακυβεύεται η ασφάλεια των ήδη λειτουργούντων συστημάτων και χωρίς να απαιτείται απότομη αντικατάσταση των υφιστάμενων μηχανισμών [5].

Τυποποίηση και διεθνή πρότυπα (standardization). Ιδιαίτερη έμφαση δίδεται επίσης στη θέσπιση διεθνών προτύπων για την κβαντοανθεκτική κρυπτογράφηση, υπό την καθοδήγηση φορέων όπως το National Institute of Standards and Technology (NIST). Η διαδικασία αυτή, γνωστή ως Post-Quantum Cryptography Standardization, στοχεύει στη δημιουργία ενιαίων προδιαγραφών, οι οποίες θα διασφαλίζουν τη συμβατότητα των εφαρμογών blockchain με τις νέες τεχνολογίες και θα διευκολύνουν την ασφαλή μετάβαση σε μελλοντικά συστήματα [5].

Σε τελική ανάλυση, η αλληλεπίδραση ανάμεσα στην κβαντική υπολογιστική και την ασφάλεια των κατανεμημένων λογιστικών βιβλίων αποτελεί πεδίο εντατικής επιστημονικής διερεύνησης, καθώς η επιτυχής αντιμετώπιση των μελλοντικών κινδύνων θεωρείται καταλυτικός παράγοντας για τη βιωσιμότητα των αποκεντρωμένων τεχνολογιών σε μακροχρόνιο ορίζοντα.

7. Συμπεράσματα & Επίλογος

Η παρούσα διπλωματική εργασία διερεύνησε σε βάθος τη συμβολή της τεχνολογίας blockchain στην ενίσχυση της ασφάλειας και της ιδιωτικότητας των αρχιτεκτονικών fog και edge computing. Η ανάλυση ανέδειξε τον τρόπο με τον οποίο τα αποκεντρωμένα καθολικά, οι μηχανισμοί συναίνεσης και τα έξυπνα συμβόλαια μπορούν να αντιμετωπίσουν τις αυξανόμενες προκλήσεις ασφαλείας σε κατανεμημένα περιβάλλοντα χαμηλής καθυστέρησης. Η σύνθεση των προηγούμενων κεφαλαίων έδειξε ότι το blockchain δεν αποτελεί απλώς μια τεχνολογία αποθήκευσης συναλλαγών αλλά ένα ισχυρό θεμέλιο για τη δημιουργία συστημάτων υψηλής ανθεκτικότητας και διαφάνειας.

7.1. Συνεισφορά της Διπλωματικής και Οφέλη

Η εργασία κατέγραψε και ταξινόμησε τα κρίσιμα ζητήματα ασφάλειας και ιδιωτικότητας που εμφανίζονται στα fog και edge περιβάλλοντα, παρουσιάζοντας συγκεκριμένες κατηγορίες επιθέσεων, τρωτοτήτων και λειτουργικών κινδύνων. Η συμβολή της εργασίας έγκειται στη συστηματική ομαδοποίηση αυτών των προβλημάτων και στη σύνδεσή τους με στοχευμένες λύσεις βασισμένες στο blockchain. Παράλληλα, τεκμηριώθηκε ο τρόπος με τον οποίο μηχανισμοί, μοντέλα και πολιτικές που απορρέουν από τη χρήση του blockchain, όπως η αμετάβλητη καταγραφή, η αποκεντρωμένη εμπιστοσύνη και οι αυτοματοποιημένες πολιτικές ασφαλείας, μπορούν να ενσωματωθούν τόσο στο fog όσο και στο edge computing, δημιουργώντας ένα συνεκτικό πλαίσιο προστασίας.

Επιπλέον, η εργασία δεν περιορίστηκε μόνο στην αποτύπωση των πλεονεκτημάτων του blockchain, αλλά ανέδειξε και τις βασικές προκλήσεις που συνοδεύουν την εφαρμογή του στα fog/edge περιβάλλοντα, όπως ζητήματα απόδοσης, καθυστέρησης, ενεργειακής κατανάλωσης, αποθήκευσης, ασφάλειας, ιδιωτικότητας συναλλαγών και κβαντικής ανθεκτικότητας. Στο πλαίσιο αυτό, καταγράφηκαν και οργανώθηκαν οι κύριες ερευνητικές κατευθύνσεις που προτείνονται στη βιβλιογραφία για την αντιμετώπιση των προκλήσεων αυτών, όπως ελαφρύτεροι μηχανισμοί συναίνεσης, τεχνικές off-chain και sharding, μηχανισμοί προστασίας έξυπνων συμβολαίων, privacy-preserving κρυπτογραφικές τεχνικές και post-quantum προσεγγίσεις. Με τον τρόπο αυτό, η εργασία συνεισφέρει όχι μόνο στην κατανόηση της παρούσας κατάστασης του πεδίου, αλλά και στη χαρτογράφηση των μελλοντικών ερευνητικών προοπτικών του.

Η εργασία ωφέλησε τον ερευνητικό χώρο συγκεντρώνοντας τη σύγχρονη βιβλιογραφία των επιλεγμένων άρθρων από τη συστηματική ανασκόπηση [1]–[17] και δημιουργώντας ένα ενιαίο θεωρητικό υπόβαθρο που επιτρέπει την καλύτερη κατανόηση των δυνατοτήτων του blockchain σε πολλαπλά επίπεδα: προστασία δεδομένων, καταγραφή γεγονότων, ταυτοποίηση κόμβων, έλεγχο

πρόσβασης και διαχείριση ιδιωτικότητας. Επίσης, αναδείχθηκαν τα πλεονεκτήματα των δημόσιων, ιδιωτικών, consortium και υβριδικών blockchains, καθώς και τα όρια κάθε προσέγγισης, με βάση τις πηγές [8], [9], [10].

7.2. Εμπειρία που Αποκομίστηκε από την Ακπόνηση της Διπλωματικής

Η διαδικασία συγγραφής οδήγησε στην ανάπτυξη σημαντικών δεξιοτήτων, όπως η ενδελεχής αναζήτηση και αξιολόγηση επιστημονικών άρθρων, η κατάρτιση δομημένης μεθοδολογίας βιβλιογραφικής ανασκόπησης, ο συνδυασμός διαφορετικών τεχνολογικών τομέων (blockchain, fog, edge computing) και η παραγωγή κριτικής ακαδημαϊκής ανάλυσης. Μέσα από τη μελέτη των βιβλιογραφικών πηγών [1]–[17], αποκτήθηκε ουσιαστική κατανόηση τόσο των τεχνικών λειτουργιών των αποκεντρωμένων δικτύων όσο και των πρακτικών δυσκολιών ενσωμάτωσής τους σε πραγματικά περιβάλλοντα.

Παράλληλα ενισχύθηκε η ικανότητα διαχείρισης σύνθετων τεχνολογικών θεμάτων, η δυνατότητα αποτίμησης διαφορετικών αρχιτεκτονικών λύσεων και η εμπειρία στην τεκμηριωμένη παρουσίαση συμπερασμάτων με επιστημονικό τρόπο. Η διαδικασία συνέβαλε επίσης στην καλύτερη κατανόηση των περιορισμών, των εμποδίων και των απαιτήσεων που συνοδεύουν την ανάπτυξη συστημάτων υψηλής ασφάλειας.

7.3. Βασικά Συμπεράσματα από τις Αναλύσεις

Η μελέτη κατέδειξε ότι τα fog και edge συστήματα, αν και προσφέρουν χαμηλή καθυστέρηση και τοπική επεξεργασία, είναι εκτεθειμένα σε πολλές επιθέσεις και τρωτότητες, όπως πλαστοπροσωπία κόμβων, χειρισμό δεδομένων, επιθέσεις σε κανάλια επικοινωνίας και παραβιάσεις ιδιωτικότητας, όχι μόνο λόγω της πολυπλοκότητας των ετερογενών συσκευών αλλά και εξαιτίας της γεωγραφικής διασποράς και φυσικής έκθεσης κόμβων, της δυναμικής ένταξης/αποχώρησης (με αδύναμες διαδικασίες onboarding), της έλλειψης ενιαίας διακυβέρνησης σε multi-domain περιβάλλοντα, των δυσκολιών συνεπούς ενημέρωσης/patching και της συχνής έκθεσης ανασφαλών διαχειριστικών διεπαφών (APIs/dashboards) στο δίκτυο, καθώς και των περιορισμών πόρων (CPU/μνήμη/ενέργεια) που συχνά οδηγούν σε “ελαφρύτερες” υλοποιήσεις ασφάλειας ή καθυστερημένη εφαρμογή μηχανισμών προστασία [2], [5]. Επιπλέον, η αποκέντρωση των κόμβων, ενώ βελτιώνει την απόδοση, αυξάνει τα σημεία εισόδου για επιθέσεις, δημιουργώντας ανάγκη για μηχανισμούς αυξημένης διαφάνειας και ισχυρής αυθεντικοποίησης.

Στο πλαίσιο αυτό, το blockchain αναδείχθηκε εξαιρετικά αποτελεσματικό ως μέσο ενίσχυσης της ασφάλειας. Οι μηχανισμοί αμετάβλητης καταγραφής εγγυώνται ότι τα γεγονότα και δεδομένα δεν μπορούν να αλλοιωθούν εκ των υστέρων [1], η κατανεμημένη συναίνεση εξουδετερώνει τις επιθέσεις σε κεντρικά σημεία [4], ενώ τα έξυπνα συμβόλαια επιτρέπουν την

αυτοματοποιημένη επιβολή πολιτικών ασφαλείας [4], [5]. Σημαντική είναι επίσης η συμβολή κρυπτογραφικών πρακτικών, όπως οι μηδενικές αποδείξεις (ZKP), η διαφορική ιδιωτικότητα και η ομοσπονδιακή μάθηση, που ενισχύουν τη διαχείριση προσωπικών δεδομένων χωρίς αποκάλυψη ταυτότητας [7], [9], [11].

Αναδείχθηκαν επίσης οι σημαντικότερες προκλήσεις που απαιτούν περαιτέρω έρευνα: η βελτίωση της κλιμακωσιμότητας των blockchains [4], η διαλειτουργικότητα μεταξύ διαφορετικών αλυσίδων και συστημάτων, η ελάττωση του ενεργειακού κόστους των μηχανισμών συναίνεσης, η συμμόρφωση με τον GDPR και η δυνατότητα ασφαλούς λειτουργίας σε ετερογενή περιβάλλοντα fog/edge με μεταβαλλόμενη ροή δεδομένων.

7.4. Ερευνητικές Κατευθύνσεις και Τελική Αποτίμηση

Η σύζευξη blockchain – fog/edge computing παρουσιάζει σημαντικές δυνατότητες, ειδικά σε εφαρμογές όπως έξυπνες πόλεις, υγειονομική περίθαλψη, έξυπνα δίκτυα ενέργειας και βιομηχανικές αλυσίδες. Μελλοντικές κατευθύνσεις περιλαμβάνουν την ανάπτυξη ενεργειακά αποδοτικών αλγορίθμων συναίνεσης [5], την ενίσχυση των cross-chain μηχανισμών, την υιοθέτηση μοντέλων blockchain με χαμηλό latency για edge εφαρμογές, καθώς και τη σύζευξη με τεχνητή νοημοσύνη για αυτοματοποιημένο εντοπισμό απειλών [12], [13]. Σημαντική είναι επίσης η συμβολή τεχνικών προστασίας ιδιωτικότητας. Οι μηδενικές αποδείξεις (ZKPs) αποτελούν ήδη ώριμη τεχνολογία σε παραγωγικά blockchain (π.χ. Zcash και zk-rollups), ενώ προσεγγίσεις όπως η διαφορική ιδιωτικότητα και η ομοσπονδιακή μάθηση—ιδίως όταν συνδυάζονται με blockchain για έλεγχο συμμετοχής, κίνητρα και ιχνηλασιμότητα—αποτελούν κυρίως ενεργές ερευνητικές/πιλοτικές κατευθύνσεις για fog/edge περιβάλλοντα. [2] [5] [7] [9] [18].

Στο σύνολο της, η εργασία καταδεικνύει ότι η πλήρης αξιοποίηση του blockchain σε fog και edge περιβάλλοντα μπορεί να δημιουργήσει ένα νέο επίπεδο ασφάλειας, διαφάνειας και αξιοπιστίας στις κατανεμημένες υποδομές. Η τεχνολογία συνεχίζει να εξελίσσεται δυναμικά και απαιτεί διεπιστημονική συνεργασία, προκειμένου οι λύσεις να καταστούν πρακτικές, ανθεκτικές και συμβατές με τις απαιτήσεις της σύγχρονης ψηφιακής οικονομίας.

8. Βιβλιογραφία

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] M. Chiang and T. Zhang, "Fog and IoT: An Overview of Research Opportunities," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 854–864, Dec. 2016. [Online]. Available: https://arxiv.org/pdf/1601.00835

[3] Yaqoob, E. Ahmed, M. H. ur Rehman, A. I. A. Ahmed, M. A. Alam, M. Imran, and M. Guizani, "The Rise of Edge Computing: A Comprehensive Survey," *IEEE Access*, vol. 7, pp. 173, 2019. [Online]. Available: https://arxiv.org/pdf/1906.08452

[4] M. Pilkington, "Blockchain Technology: Principles and Applications," in *Research Handbook on Digital Transformations*, F. X. Olleros and M. Zhegu, Eds. Edward Elgar Publishing, 2016, pp. 225–253. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2662660

[5] I. Abrar and J. A. Sheikh, "Current Trends of Blockchain Technology: Architecture, Applications, Challenges, and Opportunities," *Discover Internet of Things*, vol. 4, article 7, July 2024. [Online]. Available: https://link.springer.com/article/10.1007/s43926-024-00058-5

[6] S. Underwood, "Blockchain Beyond Bitcoin," *Communications of the ACM*, vol. 59, no. 11, pp. 15–17, Nov. 2016. [Online]. Available: https://cacm.acm.org/magazines/2016/11/209132-blockchain-beyond-bitcoin/fulltext

[7] STL Partners, "5 Blockchain Healthcare Use Cases," STL Partners, 2020. [Online]. Available: https://stlpartners.com/articles/digital-health/5-blockchain-healthcare-use-cases/

[8] Blockchain Council, "Types of Blockchains Explained: Public vs Private vs Consortium," [Online]. Διαθέσιμο: https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/

[9] Blockchain Research Lab, "Public Versus Private Blockchains," Working Paper No. 14, 2020. [Online]. Διαθέσιμο: https://www.blockchainresearchlab.org/wp-content/uploads/2020/05/BRL-Working-Paper-No-14-Public-vs-Private-Blockchains.pdf

[10] O. Dib, K.-L. Brousmiche, A. Durand, E. Thea, and E. B. Hamida, “Consortium Blockchains: Overview, Applications and Challenges,” International Journal on Advances in Telecommunications, vol. 11, no. 1 & 2, pp. 51–64, 2018. [Online]. Διαθέσιμο: https://www.thinkmind.org/articles/tele_v11_n12_2018_5.pdf

[11] S. Mohammed and N. R. Panda, "Block Chain Technology in the Pharmaceutical Supply Chain: Enhancing Transparency and Security," *International Journal for Research in Applied Science & Engineering Technology (IJRASE)*, vol. 12, no. VIII, pp. 1336-1340, Aug. 2024. [Online]. Διαθέσιμο: https://doi.org/10.22214/ijraset.2024.64117

[12] Sazu, Mesbaul & Jahan, Sakila. (2022). Impact of blockchain-enabled analytics as a tool to revolutionize the banking industry. Data Science in Finance and Economics. 2. 298-316. 10.3934/DSFE.2022014.

[13] Resource Utilization for IoT Oriented Framework Using Zero Hour Policy - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/High-level-view-of-Cloud-Fog-computing-architecture_fig1_354062176

[14] https://www.seaflux.tech/blogs/edge-fog-cloud-computing

[15] https://www.linkedin.com/pulse/difference-between-edge-fog-cloud-computing-seaflux-tech-w0fmf/

[16] Cao, Hung & Wachowicz, M. & Renso, Chiara & Carlini, Emanuele. (2019). Analytics Everywhere: Generating Insights From the Internet of Things. IEEE Access. 7. 71749-71769. 10.1109/ACCESS.2019.2919514. https://www.researchgate.net/figure/The-proposed-edge-fog-cloud-architecture_fig1_333438248

[17] Q.-V. Pham, F. Fang, V. N. Ha, M. J. Piran, M. Le, L. B. Le, W.-J. Hwang, and Z. Ding, "A Survey of Multi-Access Edge Computing in 5G and Beyond: Fundamentals, Technology Integration, and State-of-the-Art," IEEE Communications Surveys & Tutorials, 2019. [Online]. Available: https://arxiv.org/pdf/1906.08452

[18] Murtaza, M. H., Alizai, Z. A., & Iqbal, Z. (2019). *Blockchain-Based Anonymous Voting System Using zkSNARKs.* 2019 International Conference on Applied and Engineering Mathematics (ICAEM), Taxila, Pakistan, pp. 209-214. doi: 10.1109/ICAEM.2019.8853836. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8853836&isnumber=8853652.

[19] B. Kitchenham, “Procedures for Performing Systematic Reviews,” Keele University, Keele, U.K., Technical Report TR/SE-0401, 2004. [Online]. Available: https://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf

[20] B. Kitchenham and S. Charters, “Guidelines for Performing Systematic Literature Reviews in Software Engineering,” EBSE Technical Report EBSE-2007-01, 2007. [Online]. Available: https://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf

[21] V. Buterin, “A Next-Generation Smart Contract and Decentralized Application Platform,” *Ethereum White Paper*, 2014. [Online]. Available: https://ethereum.org/en/whitepaper/

[22] Hyperledger Foundation, “Hyperledger Fabric Documentation.” [Online]. Available: https://hyperledger-fabric.readthedocs.io/

[23] R3, “Corda Platform Overview.” [Online]. Available: https://www.r3.com/corda-platform/

[24] ConsenSys, “Quorum Blockchain Platform.” [Online]. Available: https://consensys.net/quorum/

[25] Ripple, “RippleNet Overview.” [Online]. Available: https://ripple.com/ripplenet/

[26] Dragonchain, “Dragonchain Overview.” [Online]. Available: https://dragonchain.com/

[27] IBM, “IBM Blockchain Platform.” [Online]. Available: https://www.ibm.com/blockchain/platform

[28] I. Miers, C. Garman, M. Green, and A. D. Rubin, “Zerocoin: Anonymous Distributed E-Cash from Bitcoin,” *IEEE Symposium on Security and Privacy (S&P)*, 2013. [Online]. Available: https://ieeexplore.ieee.org/document/6547123