ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
& ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Πρόσβαση σε Δίκτυα Βασισμένα σε Blockchain

του

Σαχινίδη Α. Θεόφιλου

Επιβλέποντες Καθηγητές:
Δρ. Σαρηγιαννίδης Παναγιώτης
Δρ. Μπουλογεώργος Αλέξανδρος – Απόστολος

Κοζάνη, Ιούλιος 2021

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
& ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Πρόσβαση σε Δίκτυα Βασισμένα σε Blockchain

του

Σαχινίδη Α. Θεόφιλου

Επιβλέποντες Καθηγητές:
Δρ. Σαρηγιαννίδης Παναγιώτης
Δρ. Μπουλογεώργος Αλέξανδρος – Απόστολος

Κοζάνη, Ιούλιος 2021

Περίληψη

Τις τελευταίες δεκαετίες, η εξέλιξη των ασύρματων τηλεπικοινωνιακών συστημάτων είναι ραγδαία και μαρτυρείται από τη διαρκή βελτίωση των προσφερόμενων υπηρεσιών και την εισαγωγή άλλων καινοτόμων. Παράλληλα αυξάνεται η πολυπλοκότητα του δικτύου και οι προκλήσεις που χρήζουν αντιμετώπισης. Ιδιαίτερα για τα B5G, σε αυτές συγκαταλέγονται ζητήματα ασφάλειας, μυστικότητας και ακεραιότητας των αποθηκευμένων ή ανταλλασσόμενων δεδομένων. Καθοριστική αναμένεται η συμβολή μιας επαναστατικής τεχνολογίας, του blockchain. Πρόκειται για ένα κατανεμημένο σύστημα βάσης δεδομένων, το οποίο αποσκοπεί στην εκτέλεση διαδικτυακών συναλλαγών, χωρίς την ανάγκη μεσολάβησης έμπιστης οντότητας, καθώς δύναται να εγγυηθεί την ασφάλεια και την ακεραιότητα των δεδομένων σε ένα P2P δίκτυο. Το blockchain, αν και ξεκίνησε ως τεχνολογία υποδομής συστημάτων εκτέλεσης συναλλαγών με ψηφιακά νομίσματα, τελευταία ενσωματώνεται σε ολοένα και περισσότερα διαφορετικά πληροφοριακά συστήματα.

Το blockchain πρόκειται να ενσωματωθεί τόσο στο δίκτυο πρόσβασης όσο και στο δίκτυο κορμού των B5G. Η παρούσα διπλωματική εργασία πραγματεύεται την ενσωμάτωση στο δίκτυο πρόσβασης και οργανώνεται σε δύο κύριους άξονες. Ο πρώτος αφορά τη μελέτη της τοπολογίας ενός τέτοιου δικτύου και τη μοντελοποίησή του ως μία χρονικά ομογενή διαδικασία Markov. Ακόμα με την εκτέλεση κατάλληλων προσομοιώσεων, γίνεται αποτίμηση των επιδόσεων του συστήματος, αναφορικά με την καθυστέρηση και την πιθανότητα αναμονής αιτήματος πρόσβασης για χρονικές μονάδες που υπερβαίνουν έναν προκαθορισμένο αριθμό. Ο δεύτερος άξονας και η καινοτομία της εργασίας, αφορά την επέκταση της παραπάνω τοπολογίας για την παροχή πρόσβασης σε εκτός κάλυψης UE μέσω της ήδη συνδεδεμένης συσκευής άλλου συνδρομητή. Προσομοιώνοντας το σενάριο αυτό, κατέστη φανερό ότι είναι πρακτικά υλοποιήσιμο και η συμπεριφορά του δικτύου, ως προς τις εξεταζόμενες παραμέτρους, δεν μεταβάλλεται. Εμφανίζεται όμως επιπλέον καθυστέρηση που αποδίδεται στη διπλή χρήση του blockchain. Οπότε η προτεινόμενη τοπολογία κρίνεται καταλληλότερη για εφαρμογές που δεν χαρακτηρίζονται από υψηλές απαιτήσεις καθυστέρησης.

Λέξεις Κλειδιά: Αλυσίδα Κοινοπραξιών, Δίκτυο Ασύρματης Πρόσβασης, Επέκταση Κάλυψης, Αναμετάδοση Διπλής Αναπήδησης, Καθυστέρηση, Ασύρματα Δίκτυα της Πέμπτης και των Επερχόμενων Γενεών

Abstract

In the past few decades, wireless telecommunication systems have witnessed rapid evolution, by continuously emerging new services and improving the quality of those already offered. This results in an ever-incising complexity of the wireless networks and the appearance of many related challenges to overcome. B5G systems face, among others, the challenge of data security, privacy and integrity during storage or information exchange. A promising solution to this problem is the integration of disruptive blockchain technology into modern cellular networks. Blockchain is a public database, characterized by security, immutability and privacy, making possible transactions among untrusted nodes of a peer-to-peer network, without the mediation of a trusted third party. Blockchain has emerged as the technology implementing cryptocurrency platforms, such as Bitcoin, but recently it is integrated with many other software products, with a different purpose.

The integration of blockchain will probably take place at both the radio access network and core network. The present diploma thesis focuses on the first case and consists of two main parts. The first one is dedicated to the study of the related topology, which is modelled as a time-homogeneous Markov process. Also, the performance of the network is assessed, in terms of latency and waiting probability, with the execution of related simulations. The second part presents the novelty of this thesis, which is the extension of the aforementioned topology to provide intermediate access to an out of coverage device. Thus, this device can access the network, through the connected device of a subscriber, who has the corresponding rights. Simulating this scenario, it became clear that the behaviour of the system regarding the key performance indicators used before is the same. But there is an extra latency, because of the double use of blockchain. So, it can be clear that the proposed topology is feasible and can be beneficial to many latency insensitive services.

Keywords: Blockchain, Radio Access Networks, Coverage Expansion, Dual-hop Relaying, Latency, Beyond 5G Networks

Δήλωση Πνευματικών Δικαιωμάτων

Δηλώνω ρητά ότι, σύμφωνα με το άρθρο 8 του Ν. 1599/1986 και τα άρθρα 2,4,6 παρ. 3 του Ν. 1256/1982, η παρούσα Διπλωματική Εργασία με τίτλο " Πρόσβαση σε Δίκτυα Βασισμένα σε Blockchain" καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας και αναφέρονται ρητώς μέσα στο κείμενο που συνοδεύουν, και η οποία έχει εκπονηθεί στο Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Δυτικής Μακεδονίας, υπό την επίβλεψη του μέλους του Τμήματος κ. Σαρηγιαννίδη Παναγιώτη αποτελεί αποκλειστικά προϊόν προσωπικής εργασίας και δεν προσβάλλει κάθε μορφής πνευματικά δικαιώματα τρίτων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή / και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα. Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και μόνο.

Υπογραφή Φοιτητή:

Ευχαριστίες

Η ολοκλήρωση της εκπόνησης της παρούσας διπλωματικής εργασίας σηματοδοτεί το πέρας της φοίτησής μου στο Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, του Πανεπιστημίου Δυτικής Μακεδονίας, στην πόλη της Κοζάνης. Τη στιγμή αυτή τα συναισθήματα είναι ανάμεικτα. Η χαρά που συνοδεύει την επιτυχία μου είναι μεγάλη, όπως και ο ενθουσιασμός που απορρέει από το γεγονός ότι η ώρα που θα εργαστώ στον τομέα που επέλεξα και αγάπησα πλησιάζει. Από την άλλη λυπάμαι, καθώς ένα όμορφο, γεμάτο γνώσεις και εμπειρίες ταξίδι έφτασε στο τέλος του. Θα ήθελα λοιπόν να ευχαριστήσω τους γονείς μου για την οικονομική στήριξη, τις συμβουλές και τη συμπαράσταση που μου προσέφεραν καθ' όλη τη διάρκεια της φοιτητικής μου ζωής. Επίσης ευχαριστώ τους φίλους μου, καθώς συνέβαλλαν ώστε η περίοδος αυτή, να αποτελέσει μία από τις ομορφότερες της ζωής μου.

Επιπλέον, θα ήθελα να ευχαριστήσω τους διδάσκοντες του Τμήματος Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών και ιδιαίτερα αυτούς που συνέβαλαν στην ολοκλήρωση της παρούσας εργασίας. Συγκεκριμένα, ευχαριστώ τον Καθηγητή Δρ. Παναγιώτη Σαρηγιαννίδη για την υποστήριξή του και την εμπιστοσύνη που έδειξε στο πρόσωπό μου, όπως και τον Δρ. Αλέξανδρο – Απόστολο Μπουλογεώργο, για τις ιδέες και την πολύτιμη καθοδήγησή του.

Περιεχόμενα

Κατάλογος Εικόνων

Συντομογραφίες

1G: First Generation (Cellular Networks)

2G: Second Generation (Cellular Networks)

3G: Third Generation (Cellular Networks)

4G: Forth Generation (Cellular Networks)

5G: Fifth Generation (Cellular Networks)

6G: Sixth Generation (Cellular Networks)

AI: Artificial Intelligence

AP: Access Point

B5G: Beyond Fifth Generation (Cellular Networks)

BCoT: Blockchain Cloud of Things

BDMA: Beam Division Multiple Access

BN: Blockchain Network

B-RAN: Blockchain Radio Access Network

CC: Cloud Computing

CN: Core Network

CoT: Cloud of Things

D2D: Device to Device

DH-BRAN: Dual Hop Blockchain RAN

DL: Distributed Ledger

EC: Edge Computing

eMBB: enhanced Mobile Broadband

EN: Edge Node

FIFO: First In First Out

FSCD: Fast Smart Contract Deployment

GSM: Global Systems for Mobile Communications

HSS: Home Subscriber Server

IIot: Industrial IoT

IoE: Internet of Everything

IoT: Internet of Things

IP: Internet Protocol

IUE: Intermediate UE

KPI: Key Performance Indicator

L5GO: Local 5G Operator

LTE: Long Term Evolution

ML: Machine Learning

mMIMO: massive Multiple Input Multiple Output

mMTC: Massive machine type communications

mmWaves: millimetre Waves

NB-IoT: Narrowband IoT

NFV: Network Functions Virtualization

NS: Network Slicing

P2P: Peer to Peer

PBFT: Practical Byzantine Fault Tolerance

PoD: Proof of Device

PoS: Proof of Stake

PoW: Proof of Work

QoE: Quality of Experience

QoS: Quality of Service

RAN: Radio Access Network

SCaaS: Small-Cell-as-a-Service

SDN: Software Defined Network

SLA: Service Level Agreement

SMS: Short Messaging Service

SON: Shelf Organized Network

TCP: Transfer Control Protocol

UE: User Equipment

UMTS: Universal Mobile Telecommunications System

URLLC: Ultra-Reliable and Low Latency Communications

1. Εισαγωγή

1.1 Κίνητρο, Πρωτοτυπία και Συνεισφορά Διπλωματικής Εργασίας

Τις τελευταίες δεκαετίες η εξέλιξη των ασύρματων τηλεπικοινωνιακών συστημάτων είναι ραγδαία και μαρτυρείται από τη συνεχή βελτίωση της ποιότητας των παρεχόμενων υπηρεσιών, αλλά και τη διαρκή εισαγωγή νέων [1]. Πρόσφατο κομβικό σημείο της εξέλιξης αυτής υπήρξε η υιοθέτηση του Διαδικτύου των Πραγμάτων (Internet of Things – IoT) [2] από τα Κυψελωτά Συστήματα Κινητών Επικοινωνιών Τέταρτης Γενιάς (Fourth Generation – 4G). Η αξιοποίηση και οι δυνατότητές του αναμένεται να διευρυνθούν από τα αντίστοιχα δίκτυα της πέμπτης και των επερχόμενων γενεών (Beyond 5G – B5G), επηρεάζοντας σημαντικά ποικίλες πτυχές της ανθρώπινης ζωής. Με την ωρίμανση και την ευρεία χρήση του IoT, ο κύριος όγκος της τηλεπικοινωνιακής κίνησης, που συνεχώς αυξάνεται, θα προέρχεται από την αυτόνομη και αυτόματη επικοινωνία μεταξύ ετερογενών έξυπνων συσκευών και αισθητήρων, αντί της τηλεφωνικής ή διαδικτυακής επικοινωνίας μεταξύ των ανθρώπων, όπως συνέβαινε μέχρι πρότινος. Αυτό δημιουργεί αρκετές προκλήσεις και βαθμιαία αυξάνει την πολυπλοκότητα της αρχιτεκτονικής των σύγχρονων κυψελωτών τηλεπικοινωνιακών δικτύων.

Βασική πρόκληση αποτελεί η επίτευξη υψηλού επιπέδου ασφάλειας, μυστικότητας και ακεραιότητας των δεδομένων που διατηρούνται στις IoT συσκευές ή ανταλλάσσονται μέσω των τηλεπικοινωνιακών συστημάτων. Η Αλυσίδα Κοινοπραξιών (Blockchain) είναι μία σχετικά νέα, πολλά υποσχόμενη και ανατρεπτική τεχνολογία που αναμένεται να συμβάλει καθοριστικά στην εκπλήρωση του στόχου αυτού. Πρόκειται για ένα δημόσιο σύστημα βάσης δεδομένων που επιτρέπει την ασφαλή επικοινωνία μεταξύ οντοτήτων ενός ομότιμου δικτύου, διασφαλίζοντας αλγοριθμικά την ακεραιότητα και τη μυστικότητα των ανταλλασσόμενων δεδομένων. Με τον τρόπο αυτό εξαλείφεται η ανάγκη μεσολάβησης κάποιας κεντρικής οντότητας. Τελευταία διεξάγονται συστηματικές ερευνητικές προσπάθειες ενσωμάτωσής του, μεταξύ άλλων, σε αρκετά διαφορετικά σημεία των ασύρματων τηλεπικοινωνιακών συστημάτων [3].

Καίριο σημείο ενσωμάτωσης είναι το Δίκτυο Ασύρματης Πρόσβασης (Radio Access Network – RAN), καθώς πρέπει να ανασχεδιαστεί, βασιζόμενο σε υψηλά πρότυπα ασφάλειας και εμπιστευτικότητας. Οπότε θα καταφέρει να διαχειριστεί το διαρκώς αυξανόμενο πλήθος και την ετερογένεια των Συνδρομητικών Εξοπλισμών (User Equipments – UEs) που συνδέονται ταυτόχρονα σε αυτό. Προτείνεται λοιπόν η αρχιτεκτονική του Ασύρματου Δικτύου Πρόσβασης βασιζόμενο σε Αλυσίδα Κοινοπραξιών (Blockchain Radio Access Network – B-RAN) [4], που

αποτελεί το αντικείμενο μελέτης της παρούσας διπλωματικής εργασίας. Πιο συγκεκριμένα, εξετάζεται η τοπολογία του και το πρωτόκολλο σύνδεσης ενός UE σε αυτό, ενώ παρουσιάζεται διεξοδικά το μοντέλο Markov ομογενούς χρόνου που περιγράφει το δίκτυο, με την αξιοποίηση της θεωρίας ουρών αναμονής. Κατόπιν γίνεται αποτίμηση των επιδόσεων του συστήματος, μέσω προσομοιώσεων, οπότε εξετάζεται η μεταβολή της καθυστέρησης και της πιθανότητας παραμονής αιτήματος πρόσβασης σε ουρά, για περισσότερες χρονικές μονάδες από ένα δεδομένο κατώφλι, με τη μεταβολή σημαντικών παραμέτρων λειτουργίας του δικτύου.

Η πρωτοτυπία της εργασίας έγκειται στην επέκταση της παραπάνω ανάλυσης οπότε και εξασφαλίζεται η έμμεση πρόσβαση σε UE, που βρίσκεται σε περιοχή εκτός δικτυακής κάλυψης. Αυτό επιτυγχάνεται με τη μεσολάβηση της συσκευής ενός άλλου συνδρομητή (Intermediate UE – IUE), ο οποίος διαθέτει το δικαίωμα παροχής της συγκεκριμένης υπηρεσίας και εξοπλισμό με επαρκείς δυνατότητες. Η τοπολογία αυτή ονομάστηκε Δίκτυο Ασύρματης Πρόσβασης Διπλής Αναπήδησης βασισμένο σε Αλυσίδα Κοινοπραξιών (Dual Hop Blockchain RAN – DH-BRAN). Κατ' αντιστοιχία με την προηγούμενη ανάλυση, προτείνεται το πρωτόκολλο πρόσβασης στο DH-BRAN και στη συνέχεια, αυτό μοντελοποιείται ως μία διαδικασία Markov. Τέλος, με την επέκταση των προαναφερόμενων προσομοιώσεων για το σενάριο της έμμεσης πρόσβασης, επιβεβαιώνεται η δυνατότητα της πρακτικής υλοποίησης του συγκεκριμένου πρωτοκόλλου και γίνεται αποτίμηση των επιδόσεών του.

1.2 Δομή Διπλωματικής Εργασίας

Η παρούσα διπλωματική εργασία, εκτός από την εισαγωγή η οποία αποτελεί το πρώτο κεφάλαιο, δομείται και από άλλα πέντε κεφάλαια:

- Στο δεύτερο κεφάλαιο παρατίθεται το θεωρητικό υπόβαθρο του blockchain. Πιο συγκεκριμένα αναλύεται διεξοδικά η δομή και η λειτουργία των δικτύων blockchain, όπως και η έννοια των έξυπνων συμβολαίων. Επίσης γίνεται αναφορά στα είδη των συστημάτων blockchain και στις σημαντικότερες κατηγορίες λογισμικών όπου αυτά βρίσκουν εφαρμογή.
- Στο τρίτο κεφάλαιο αναφέρονται τα βασικά χαρακτηριστικά των σύγχρονων τηλεπικοινωνιακών συστημάτων και οι πιθανότερες εξελίξεις που αναμένεται να συντελεστούν σε αυτά τα προσεχή έτη. Ακόμα παρουσιάζεται η ανάγκη που ωθεί στην ενσωμάτωση του blockchain σε αυτά και παρατίθεται η ανασκόπηση της σχετικής

βιβλιογραφίας, με ιδιαίτερη έμφαση στην ενσωμάτωση στο δίκτυο πρόσβασης καθώς αποτελεί και αντικείμενο της εργασίας αυτής.

- Το τέταρτο κεφάλαιο αφορά τη μελέτη της απλούστερης προτεινόμενης τοπολογίας του B-RAN ενός B5G τηλεπικοινωνιακού συστήματος και του μοντέλου Markov που την περιγράφει. Επιπλέον πραγματοποιείται αποτίμηση των επιδόσεων του δικτύου, με τη διενέργεια προσομοιώσεων.
- Στο πέμπτο κεφάλαιο, η παραπάνω ανάλυση επεκτείνεται για την περίπτωση της έμμεσης πρόσβασης, όπου μία εκτός κάλυψης συσκευή αποκτά πρόσβαση στο τηλεπικοινωνιακό σύστημα αφού πρώτα συνδεθεί στη συσκευή άλλου χρήστη.
- Το έκτο και τελευταίο κεφάλαιο αφιερώνεται στην επισήμανση των σημαντικότερων συμπερασμάτων που προέκυψαν από την εκπόνηση της εργασίας και προτείνονται πιθανές κατευθύνσεις προς τις οποίες διαφαίνονται δυνατότητες επέκτασής της.

2 Η Τεχνολογία Blockchain

Το blockchain είναι ένα είδος κατανεμημένου συστήματος βάσης δεδομένων, που παρουσιάστηκε πρώτη φορά το 2008, ως λειτουργικός πυλώνας της πρώτης εφαρμογής συναλλαγών με ψηφιακά νομίσματα (κρυπτονομίσματα), του Bitcoin [5]. Πρόκειται για μία επαναστατική τεχνολογία, καθώς συμβάλλει καθοριστικά στην πραγματοποίηση συναλλαγών μεταξύ δύο ή περισσότερων κόμβων ενός Ομότιμου Δικτύου (Peer to Peer – P2P Network) παρέχοντας ασφάλεια και ακεραιότητα των δεδομένων, χωρίς τη μεσολάβηση κάποιας έμπιστης κεντρικής οντότητας (π.χ. τραπεζικός οργανισμός). Τα τελευταία χρόνια διενεργούνται συστηματικές ερευνητικές προσπάθειες αξιοποίησης των πλεονεκτικών χαρακτηριστικών της τεχνολογίας αυτής σε πληροφοριακά συστήματα ποικίλων κατηγοριών, πράγμα που εκτιμάται ότι θα επιφέρει ριζικές αλλαγές στην καθημερινότητα των ανθρώπων.

Στο παρόν κεφάλαιο αναπτύσσεται το θεωρητικό υπόβαθρο του blockchain, όπου παρατίθενται σημαντικές γνώσεις σχετικές με τη συγκεκριμένη τεχνολογία, που αξιοποιήθηκαν κατά την εκπόνηση της παρούσας εργασίας. Αναλυτικότερα παρουσιάζεται η δομή, η λειτουργία και τα χαρακτηριστικά του blockchain και του δικτύου ομότιμων κόμβων, στο οποίο αυτό αναπτύσσεται. Επιπλέον μελετώνται τα πλεονεκτήματα που συνεπάγεται η ενσωμάτωσή του σε ποικίλα ετερογενή λογισμικά, εφ’ όσον συνδυαστεί με τα έξυπνα συμβόλαια και επιλεχθεί ο βαθμός κεντρικού ελέγχου που ταιριάζει στο εκάστοτε πληροφοριακό σύστημα.

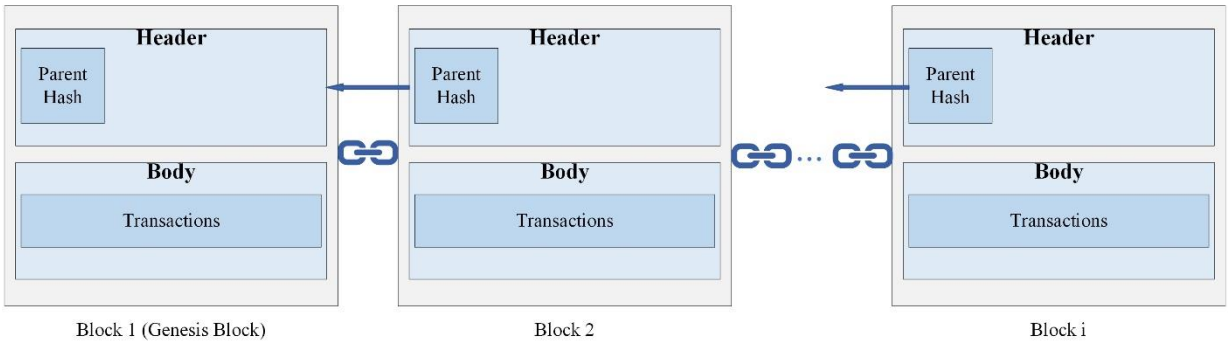
2.1 Το Δίκτυο Blockchain

Το blockchain αναπτύσσεται και λειτουργεί στο υπολογιστικό περιβάλλον ενός ομότιμου δικτύου [6], το οποίο καλείται Δίκτυο Blockchain (Blockchain Network – BN). Σχηματίζεται διασυνδέοντας υπολογιστικές μηχανές, που ονομάζονται κόμβοι (nodes), έτσι ώστε να μπορούν να επικοινωνούν ή να χρησιμοποιούν κοινούς πόρους αυτόνομα. Δηλαδή δεν απαιτείται η ύπαρξη κεντρικής υπολογιστικής οντότητας ή λογισμικού για το συντονισμό της διαδικασίας και τον έλεγχο του δικτύου.

2.1.1 Δομικά Στοιχεία

Το blockchain, όπως υποδηλώνει και το όνομά του, αποτελεί μία αλυσίδα χρονολογικά διασυνδεδεμένων blocks [3], [7] (Εικόνα 2-1). Η διασύνδεση αυτή επιτυγχάνεται με την

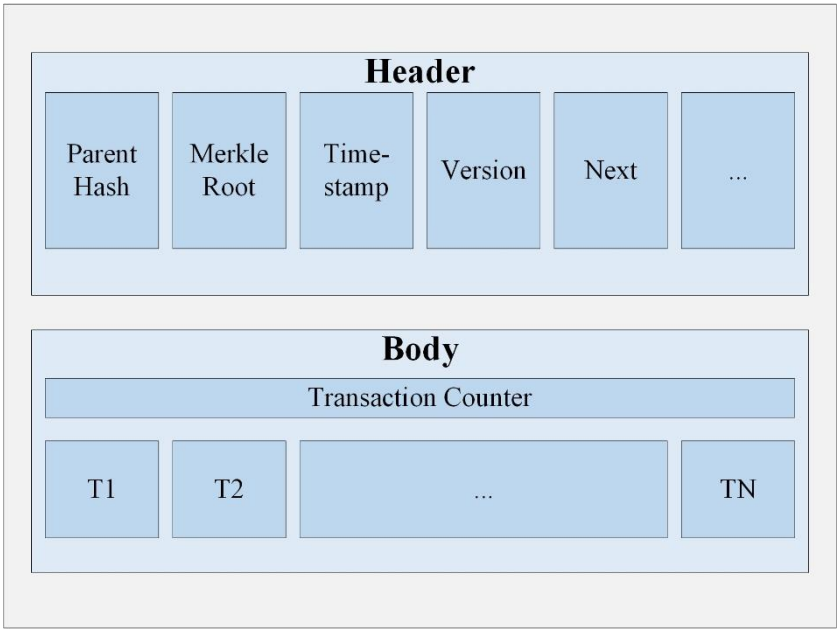
ανάθεση σε κάθε block μίας χρονικής σφραγίδας (timestamp) και μίας ετικέτας κατακερματισμού (hash label). Η πρώτη, αντιστοιχεί στην ακριβή ημερομηνία και ώρα δημιουργίας του block. Η δεύτερη είναι μία τιμή, μοναδική για κάθε block, που υπολογίζεται βάσει μίας κρυπτογραφικής συνάρτησης κατακερματισμού (hash function). Αυτή λαμβάνει ως ορίσματα, συχνά μεταξύ άλλων, δύο προϋπάρχουσες τιμές κατακερματισμού: το δείκτη της ρίζας του Merkle Tree (Merkle root) και την αντίστοιχη ετικέτα του προηγούμενου block (parent block hash). Το Merkle root προκύπτει λαμβάνοντας υπόψη τα δεδομένα των συναλλαγών που καταγράφονται στο block, ενώ μέσω του parent block hash εξασφαλίζεται η συμμετοχή της ετικέτας κατακερματισμού του αμέσως προηγούμενου block στη διαμόρφωση της αντίστοιχης τιμής του τρέχοντος. Εξαίρεση αποτελεί το εναρκτήριο block της αλυσίδας, καθώς δε συνδέεται με κάποιο πατρικό και ονομάζεται block γέννησης (genesis block). Η διαδικασία της διασύνδεσης συμβάλλει στην εγγύηση της ακεραιότητας των δεδομένων που διατηρούνται στο blockchain, μηχανισμός που εξηγείται αναλυτικότερα στη συνέχεια.



Εικόνα 2-1: Χρονολογική διασύνδεση των blocks

Ένα block δομείται από δύο κύρια μέρη (Εικόνα 2-2), την επικεφαλίδα (header) και το σώμα (body). Το τελευταίο περιλαμβάνει μία ή περισσότερες συναλλαγές, οργανωμένες σε δενδροειδή δομή δεδομένων, το Merkle Tree. Αυτές αφορούν την επικοινωνία μεταξύ δύο ή περισσότερων κόμβων του BN, που αποσκοπεί στη μεταφορά ή στο διαμοιρασμό δεδομένων, χρημάτων, υπολογιστικών πόρων ή άλλων στοιχείων. Ο μέγιστος αριθμός συναλλαγών που δύνανται να ομαδοποιηθούν σε κοινό block διαφέρει από σύστημα σε σύστημα και καθορίζεται από το μέγεθος των συναλλαγών και τη χωρητικότητα των blocks. Η επικεφαλίδα περιλαμβάνει αρκετά πεδία, ενώ η μορφή της προσδιορίζεται σημαντικά από τον χρησιμοποιούμενο αλγόριθμο ομοφωνίας, έννοια που θα αποσαφηνιστεί στη συνέχεια. Μερικά από τα πλέον συνηθισμένα πεδία της επικεφαλίδας είναι η ετικέτα κατακερματισμού του προηγούμενου

block, ο δείκτης Merkle root, η χρονική σφραγίδα και το version. Αυτό παρέχει σημαντικές πληροφορίες που σχετίζονται με το block και καθορίζει τους κανόνες επικύρωσής του. Επιπλέον, συχνή είναι η χρήση ενός πεδίου υπόδειξης του κόμβου που θα γεννήσει το επόμενο block, η μορφή του οποίου εξαρτάται από τον χρησιμοποιούμενο αλγόριθμο ομοφωνίας.



Εικόνα 2-2: Δομή block

Το άλλο βασικό δομικό στοιχείο κάθε συστήματος blockchain είναι το Κατανεμημένο Κατάστιχο (Distributed Ledger – DL) [3]. Πρόκειται για ένα είδος κατανεμημένης βάσης δεδομένων, όπου κάθε κόμβος ενός ομότιμου δικτύου, εν προκειμένω του BN, διατηρεί ένα πλήρες αντίγραφο της πληροφορίας της βάσης. Έτσι αμέσως μετά την έγκριση και εκτέλεση μίας συναλλαγής, το αντίγραφο κάθε κόμβου ενημερώνεται κατάλληλα, ενσωματώνοντας την πληροφορία που προκύπτει από αυτή. Αξίζει να σημειωθεί ότι κάθε εγγραφή στο κατανεμημένο κατάστιχο σχετίζεται με μοναδική κρυπτογραφημένη υπογραφή και χρονική σφραγίδα, καθιστώντας εξαιρετικά απίθανη την αλλοίωσή της από μη εξουσιοδοτημένους χρήστες ή κατά τη διάρκεια επιθέσεων.

2.1.2 Ασφάλεια Συστήματος Blockchain

Είναι σύνηθες τα πληροφοριακά συστήματα που συνδράμουν στις συναλλαγές μεταξύ χρηστών του διαδικτύου, τους οποίους δεν χαρακτηρίζει η αμοιβαία εμπιστοσύνη, να αξιοποιούν

κάποια κεντρική οντότητα (π.χ. τραπεζικός οργανισμός), για την υποβοήθηση βασικών λειτουργιών τους. Έτσι η διαμόρφωση των κανόνων που διέπουν μία συναλλαγή, η επιβολή και η διασφάλιση της τήρησής τους, αλλά και η εγγύηση της προστασίας από κακόβουλες ενέργειες και δικτυακές επιθέσεις λαμβάνουν χώρα κατά κύριο λόγο στις κεντρικοποιημένες υπολογιστικές μηχανές των μεσολαβούντων οντοτήτων. Ωστόσο το blockchain ως κατανεμημένο σύστημα, δε βασίζεται σε κάποια τέτοια οντότητα, οπότε το «κενό» που δημιουργείται πρέπει να καλυφθεί με την εκτέλεση κατάλληλων διαδικασιών και αλγορίθμων στους ομότιμους κόμβους του BN. Συχνά, τη βάση των λειτουργιών αυτών αποτελεί η Οικονομία Κρυπτονομισμάτων (Cryptoeconomics) [8], με την οποία η ανέντιμη συμπεριφορά καθίσταται αδύνατη ή οικονομικά ασύμφορη, έστω και υπό προϋποθέσεις, μέσω του συνδυασμού της κρυπτογραφίας με τα κατάλληλα οικονομικά κίνητρα (π.χ. αμοιβή miner για γέννηση block).

Λειτουργικός πυρήνας του blockchain είναι ο αλγόριθμος ομοφωνίας (consensus algorithm) [3], [9], [10] που εκτελείται από την πλειοψηφία, ή συχνά από το σύνολο, των κόμβων ενός BN, με σκοπό την επίτευξη συμφωνίας μεταξύ τους σχετικά με την τρέχουσα κατάσταση του δικτύου. Δηλαδή κάθε χρονική στιγμή, όλοι οι συμμετέχοντες του BN αποδέχονται την ίδια πληροφορία που διατηρείται στο DL ως ακριβή και έγκυρη. Οπότε είναι αναγκαίο κάθε κόμβος να είναι βέβαιος για την ορθότητα της προσάρτησης του τελευταίου block στην αλυσίδα, αλλά και για την εγκυρότητα και εντιμότητα των συναλλαγών που περικλείει, πράγμα που εξασφαλίζουν τα Cryptoeconomics, σε συνδυασμό με την παραχώρηση ίσων δικαιωμάτων σε κάθε κόμβο.

Η διαδικασία επιλογής του κόμβου ο οποίος θα γεννήσει το επόμενο block που θα προσαρτηθεί στο τέλος της αλυσίδας ονομάζεται εξόρυξη (mining) [11] και είναι μέρος της διαδικασίας επίτευξης ομοφωνίας. Σε αυτή μετέχει είτε το σύνολο είτε ένα υποσύνολο των κόμβων του BN, που καλούνται εξορυκτές (miners). Πιο συγκεκριμένα, κάθε φορά που κάποιο μέλος του BN επιθυμεί να εκκινήσει μία συναλλαγή, αποστέλλει (broadcast) σε κάθε miner του BN ένα αντίστοιχο αίτημα. Καθένας από αυτούς συλλέγει τέτοια αιτήματα και εφόσον είναι έγκυρα, ομαδοποιεί τις αντίστοιχες συναλλαγές σε ένα υποψήφιο block. Κατόπιν, μέσω της διαδικασίας της εξόρυξης, επιλέγεται ο κόμβος του οποίου το block θα γίνει αποδεκτό και θα αποτελέσει τον επόμενο κρίκο της αλυσίδας του blockchain.

Συχνά λόγω του mining, είναι λογικό να δημιουργείται μία κατάσταση όπου δύο ή περισσότεροι miners εξάγουν ταυτόχρονα στο δίκτυο έγκυρο block. Το αποτέλεσμα είναι η ύπαρξη πολλαπλών έγκυρων αλυσίδων, την ίδια χρονική στιγμή στο ίδιο BN, που διαφέρουν

μόνο ως προς το τελευταίο block. Στην περίπτωση αυτή, κάθε miner συνεχίζει την προσπάθειά του βασιζόμενος στο block που έχει προσαρτηθεί στη δικιά του αλυσίδα. Εν τέλει η επικρατούσα αλυσίδα είναι αυτή που ανήκει στον miner που γεννά το επόμενο block, ενώ κάθε άλλη αλυσίδα ενημερώνεται κατάλληλα. Κάθε block που δεν επικρατεί ονομάζεται ορφανό ή μπαγιάτικο block (orphan or stale block).

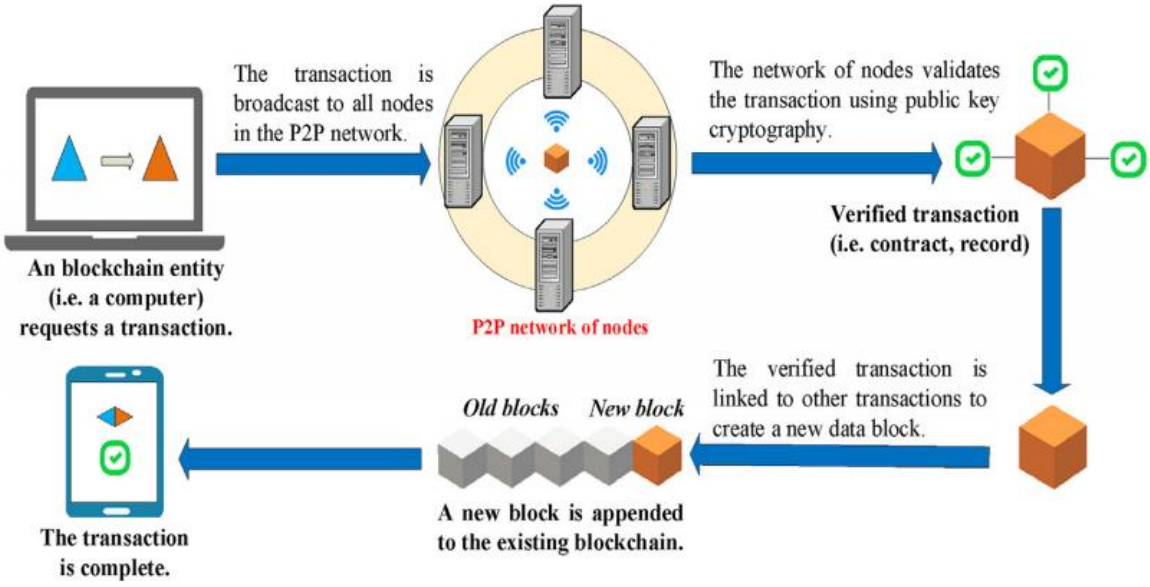
Η βασικότερη κατηγορία αλγορίθμων ομοφωνίας (και mining) είναι αυτοί που βασίζονται στα Cryptoeconomics. Σύμφωνα με την προσέγγιση αυτή, ο κόμβος που θα επιλύσει πρώτος ένα hash puzzle, δηλαδή ένα υπολογιστικά δύσκολο (πολύπλοκο) πρόβλημα, βασιζόμενο στις συναρτήσεις κατακερματισμού, είναι αυτός που θα γεννήσει το επόμενο block. Έτσι κόμβοι με μεγαλύτερη υπολογιστική ισχύ έχουν περισσότερες πιθανότητες επιλογής. Κάθε miner έχει κίνητρο να ανταγωνίζεται τους υπόλοιπους, καθώς η επιλογή του σχετίζεται με κάποια αμοιβή (mining reword). Αντίθετα, το κέρδος από πιθανή μη έντιμη συμπεριφορά είναι συνήθως μικρότερο από την αμοιβή mining, ενώ η παραγωγή «ανέντιμων» blocks, στην πλειονότητα των περιπτώσεων, ανιχνεύεται από τους υπόλοιπους miners και σε πολλά συστήματα επιβάλλονται αντίστοιχες κυρώσεις. Σε αυτήν την κατηγορία ανήκει και ο πλέον χρησιμοποιούμενος αλγόριθμος ομοφωνίας, ο Proof of Work (PoW), τον οποίο αξιοποιεί και το Bitcoin [5]. Τα τελευταία χρόνια έχουν αναπτυχθεί και άλλοι αλγόριθμοι ομοφωνίας [12], με επικρατέστερους τους Proof of Stake (PoS) και Practical Byzantine Fault Tolerance (PBFT). Στα τηλεπικοινωνιακά συστήματα και το IoT κερδίζει συνεχώς έδαφος ο Proof of Device (PoD), που βασίζεται στο μοναδικό αναγνωριστικό κάθε UE που αποκτά πρόσβαση στο δίκτυο. Κάθε αλγόριθμος παρουσιάζει διαφορετικά χαρακτηριστικά, πλεονεκτήματα και μειονεκτήματα, επομένως μπορεί να κριθεί περισσότερο ή λιγότερο κατάλληλος για κάποια εφαρμογή.

Επιπλέον κάθε BN αξιοποιεί την τεχνολογία της ψηφιακής υπογραφής [7], για την επιβεβαίωση της ταυτότητας κάποιας οντότητάς του, όποτε αυτό απαιτηθεί. Έτσι κάθε χρήστης διαθέτει ένα ζεύγος κλειδιών: ένα ιδιωτικό, το οποίο γνωρίζει αποκλειστικά ο ίδιος και ένα δημόσιο, γνωστό σε κάθε συμμετέχοντα. Προκειμένου να πραγματοποιηθεί η επαλήθευση της ταυτότητας ενός χρήστη (authentication), αυτός οφείλει να κρυπτογραφήσει (υπογράψει) τη συναλλαγή που δημιουργεί με το ιδιωτικό του κλειδί. Κατόπιν οποιοσδήποτε την αποκρυπτογραφήσει, με το δημόσιο κλειδί του συγκεκριμένου χρήστη, μπορεί να είναι βέβαιος για την ταυτότητα του αποστολέα.

2.1.3 Διαδικασία Εκτέλεσης Συναλλαγής

Η ακολουθία των ενεργειών που εκτελούνται, στην απλούστερη περίπτωση, όπου πραγματοποιείται μία συναλλαγή μεταξύ δύο μόνο κόμβων του BN παρουσιάζεται στην Εικόνα 2-3. Έστω λοιπόν ότι ένας κόμβος, ο Α, ο οποίος επιθυμεί να εκκινήσει μία μεταφορά προς έναν άλλο κόμβο, τον Β.

1. Ο κόμβος Α κοινοποιεί (broadcast) στο BN ένα αίτημα έναρξης συναλλαγής με τον κόμβο Β.
2. Κάθε miner λαμβάνει τη συναλλαγή, επιβεβαιώνει την ορθότητα και την εντιμότητά της, οπότε την εισάγει στο υποψήφιο block που σχηματίζει.
3. Μετά το πέρας του mining, η συναλλαγή έχει περιληφθεί στο block (δηλαδή στη δομή δεδομένων Merkle Tree) του miner που επιλέχθηκε.
4. Το απαιτούμενο ποσοστό των miners επικυρώνει το block, με την εκτέλεση του αλγόριθμου ομοφωνίας, οπότε αυτό προστίθεται στο τέλος της blockchain.
5. Τέλος, το αντίγραφο του κατάστιχου κάθε μέλους του BN ενημερώνεται με την πληροφορία που εξάγεται από τη συναλλαγή.



Εικόνα 2-3 [3]: Διαδικασία εκτέλεσης συναλλαγής σε blockchain

2.2 Έξυπνα Συμβόλαια

Η έννοια των έξυπνων συμβολαίων [3], [9], [13] εμφανίστηκε στα μέσα της δεκαετίας του 1990, από τον Szabo [14], για να περιγράψει προγράμματα που «τρέχουν» στις υπολογιστικές μηχανές ενός P2P δικτύου, συνδυάζοντας πρωτόκολλα και διεπαφή χρήστη προκειμένου να επιβάλουν τους όρους ενός συμβολαίου. Η καινοτομία τους έγκειται στην αυτόματη εκτέλεση των όρων του συμβολαίου μεταξύ των ομότιμων κόμβων και χωρίς τη μεσολάβηση κεντρικής οντότητας. Παρά τη χρησιμότητα των χαρακτηριστικών τους, η ευρεία ανάπτυξη και αξιοποίησή τους ξεκίνησε αρκετά χρόνια αργότερα, με την ωρίμανση της τεχνολογίας των BN, καθώς αποτελούν ιδανικό περιβάλλον ανάπτυξής τους.

Στις μέρες μας, ο κώδικας των έξυπνων συμβολαίων εκτελείται σχεδόν αποκλειστικά στα BNs, οπότε ο ορισμός τους περιλαμβάνει πλέον και τη συγκεκριμένη έννοια. Ορίζονται δηλαδή ως ψηφιακά σύνολα κανόνων τα οποία διαμορφώνουν, επικυρώνουν και επιβάλλουν αυτόματα, όταν πληρούνται συγκεκριμένες προϋποθέσεις, τους όρους ενός συμβολαίου που συνάπτεται μεταξύ δύο ή περισσότερων κόμβων ενός BN. Η ανάπτυξη και η εκτέλεση των έξυπνων συμβολαίων σε ένα σύστημα blockchain, καθιστά πρακτικά αδύνατη τη μη εξουσιοδοτημένη τροποποίηση του κώδικά τους, ενώ εγγυάται υψηλό επίπεδο ασφάλειας και ιδιωτικότητας, χωρίς τη μεσολάβηση κεντρικής οντότητας. Επιπλέον, ένα έξυπνο συμβόλαιο μπορεί να εκτελέσει πιο πολύπλοκες λειτουργίες με την προσθήκη ευφυίας στον κώδικά του, οπότε μπορεί να κατέχει κάποια κεφάλαια ή στοιχεία (assets) και να τα «διαχειρίζεται», παίζοντας το ρόλο ευφυούς πράκτορα.

Προγραμματιστικά, ο κώδικας ενός έξυπνου συμβολαίου έχει δύο ορίσματα, την αξία (value) και την κατάστασή (state) του. Προκειμένου να εξασφαλιστεί ακριβής, προκαθορισμένη και αυτόματη ανταπόκρισή του, αμέσως μόλις διαμορφωθούν οι προκαθορισμένες συνθήκες, αξιοποιούνται if – then δηλώσεις. Η συγγραφή του κώδικα των έξυπνων συμβολαίων γίνεται με την αξιοποίηση ειδικών γλωσσών προγραμματισμού, ενώ η εκτέλεσή του λαμβάνει χώρα σε εικονικές μηχανές που φιλοξενούνται στις υπολογιστικές μηχανές των miners.

Η προγραμματιστική ανάπτυξη και εκτέλεση των έξυπνων συμβολαίων σχετίζεται στενά με το blockchain. Αρχικά, οι όροι του συμβολαίου εγκρίνονται και υπογράφονται ψηφιακά από τους miners, παρόμοια με την έγκριση ενός αιτήματος συναλλαγής. Κατόπιν ο κώδικας περικλείεται σε ένα block, το οποίο επικυρώνεται και προσαρτάται στο τέλος της αλυσίδας. Έτσι οποιοσδήποτε χρήστης του BN το επιθυμεί, έχει τη δυνατότητα να πυροδοτήσει την εκτέλεση του έξυπνου συμβολαίου, αιτούμενος μία συναλλαγή επίκλησης (invoke transaction). Μία

συναλλαγή δημιουργίας ή επίκλησης έξυπνου συμβολαίου εκτελείται στο BN παρόμοια με μία οποιαδήποτε συναλλαγή.

2.3 Χαρακτηριστικά

Στην παρούσα υποενότητα συνοψίζονται τα πλεονεκτήματα που προσδίδει το blockchain, σε συνδυασμό με τα έξυπνα συμβόλαια, στα λογισμικά που ενσωματώνεται. Ακόμα αναλύονται σημαντικές προκλήσεις της ενσωμάτωσής του σε αρκετές εφαρμογές.

Το βασικότερο χαρακτηριστικό του blockchain είναι η **κατανεμημένη του λειτουργία (distributed)** [3], [7]. Δεν εξαρτάται δηλαδή, από κάποια έμπιστη διαμεσολαβητική οντότητα, καθώς η καταγραφή, η αποθήκευση και η ενημέρωση των δεδομένων γίνεται μεταξύ ομότιμων κόμβων. Μάλιστα, η ασφάλεια και η αξιοπιστία του συστήματος παραμένει υψηλή, παρά την έλλειψη εμπιστοσύνης μεταξύ των κόμβων, χάρη στην εκτέλεση κατάλληλων αλγορίθμων και διαδικασιών στο BN. Έτσι αυξάνεται η επίδοση του συστήματος, ενώ ταυτόχρονα μειώνεται το κόστος των συναλλαγών, αφού σε αυτό δεν προστίθεται η αμοιβή της ενδιάμεσης οντότητας, αλλά η σημαντικά μικρότερη των miners. Αποφεύγεται επίσης το μοναδικό σημείο αστοχίας (single point of failure), οπότε το σύστημα δεν καταρρέει από τυχόν βλάβες των συστημάτων της κεντρικής οντότητας ή επιθέσεις σε αυτές. Επιπλέον, επιλύεται το πρόβλημα που προκύπτει όταν η αξιοπιστία των κεντρικών οντοτήτων αποδεικνύεται κατώτερη των απαιτήσεων και των προσδοκιών.

Το blockchain εγγυάται την **ακεραιότητα (immutability)** των δεδομένων και την **ιχνηλασιμότητα (traceability)** των συναλλαγών [3]. Δηλαδή, σε ένα λογισμικό όπου αξιοποιείται το blockchain είναι εξαιρετικά δύσκολη και απίθανη η διαγραφή ή τροποποίηση των δεδομένων συναλλαγής που έχει περιληφθεί σε κάποιο block, ιδιαίτερα όταν δεν βρίσκεται στο τέλος της αλυσίδας. Αυτό επιτυγχάνεται με την ισχυρή χρονολογική διασύνδεση των blocks, μέσω των ετικετών κατακερματισμού. Στον υπολογισμό κάθε τέτοιας ετικέτας, εκτός αυτής που βρίσκεται στον εναρκτήριο «κρίκο» της αλυσίδας, λαμβάνεται υπόψη η αντίστοιχη ετικέτα του πατρικού block, με αποτέλεσμα κάθε block να επιβεβαιώνει τα προηγούμενα. Επιπλέον, στον υπολογισμό συμμετέχει και μία τιμή κατακερματισμού που προκύπτει από το σύνολο των δεδομένων του block, οπότε οποιαδήποτε μεταβολή των δεδομένων αυτών γίνεται άμεσα αντιληπτή, καθώς οδηγεί σε αλλαγή της ετικέτας του τρέχοντος αλλά και καθενός block – απογόνου. Επιπροσθέτως, τόσο κάθε block όσο και κάθε συναλλαγή λαμβάνει μία χρονική σφραγίδα, ώστε ανά πάσα στιγμή να μπορεί να επιβεβαιωθεί η ορθότητα της χρονολογικής

αλληλουχίας. Ακόμα στη διασφάλιση της ακεραιότητας, συμβάλλει και ο τρόπος ενημέρωσης κάθε αντίγραφου του DL. Έτσι για να τροποποιήσει ή να διαγράψει τα δεδομένα μίας εγγραφής (στο DL), κάποιος εξουσιοδοτημένος χρήστης, είναι υποχρεωμένος να αιτηθεί μία νέα συναλλαγή. Οπότε προκύπτει μία άλλη σημαντική ιδιότητα των συστημάτων blockchain, αυτή της ιχνηλασιμότητας των δεδομένων, καθώς μπορούν να ανακτηθούν εύκολα οι ενέργειες τροποποίησής τους, αφού είναι καταγεγραμμένες στις συναλλαγές προηγούμενων blocks.

Οι πληροφορίες που διατηρούνται στο κατανεμημένο κατάστιχο είναι ορατές από κάθε κόμβο του BN, αφού διαθέτει ένα ενημερωμένο αντίγραφό τους. Επιπλέον στις περισσότερες περιπτώσεις οι χρήστες έχουν πλήρη και κοινά δικαιώματα συμμετοχής στις διαδικασίες του mining και της επίτευξης ομοφωνίας. Χάρη στις τεχνολογίες αυτές, blocks που δεν είναι ορθά ή έγκυρα, ή ενδεχομένως περιέχουν συναλλαγές που αποσκοπούν στην κακόβουλη τροποποίηση των πληροφοριών, είναι εξαιρετικά απίθανο να γίνουν αποδεκτά από τους «έντιμους» κόμβους που τα επικυρώνουν. Με αυτούς τους τρόπους εξασφαλίζεται η **διαφάνεια (transparency)** στο blockchain.

Ένα ακόμα πλεονέκτημα του blockchain είναι η **ανωνυμία (anonymity)** [10], που εξασφαλίζεται καθώς κάθε χρήστης αλληλοεπιδρά με το BN μέσω μίας διεύθυνσης που του παραχωρείται και δεν προσδιορίζει απαραίτητα την πραγματική του ταυτότητα, μια και για την επίτευξη της ομοφωνίας δεν απαιτείται authentication. Ωστόσο οι ερευνητικές προσπάθειες βελτίωσης της ιδιωτικότητας και της ανωνυμίας του blockchain σε ορισμένες εφαρμογές συνεχίζονται. Επιπλέον ο κώδικας των περισσότερων δημόσιων blockchain είναι **διαθέσιμος (open source)** [10], πράγμα που δίνει τη δυνατότητα σε κάθε προγραμματιστή να τον βελτιώσει ή να τον ενσωματώσει στην ανάπτυξη των δικών του λογισμικών. Αξίζει να σημειωθεί μάλιστα, ότι αυτό δεν αποτελεί απειλή και δεν μειώνει την ασφάλεια του δικτύου, καθώς η αρχιτεκτονική του BN παρέχει **προστασία και από τους ιδίους τους προγραμματιστές** [15], ακριβώς με τους ίδιους μηχανισμούς που εξασφαλίζεται για κάθε άλλο χρήστη.

Εκτός από τα παραπάνω πλεονεκτήματα, από την ενσωμάτωση του blockchain σε πολλά πληροφοριακά συστήματα συχνά εμφανίζονται και αρκετές προκλήσεις, όπως η πιθανότητα επίθεσης πλειοψηφίας, η αναβάθμιση προγραμμάτων που εκτελούνται στο BN και η διαρκώς αυξανόμενη πληροφορία που αποθηκεύεται σε ένα τέτοιο σύστημα [10].

Τα blockchains, όπου κατά το mining επιλέγεται ο κόμβος που θα επιλύσει πρώτος ένα υπολογιστικά δύσκολο πρόβλημα (hash puzzle), όπως αυτά που βασίζονται στο PoW, είναι ευάλωτα σε **επιθέσεις πλειοψηφίας (Majority attacks or 51% attacks)**. Σε ένα τέτοιο σύστημα, η πιθανότητα επιλογής ενός κόμβου αυξάνεται όσο μεγαλύτερη είναι η υπολογιστική

ισχύς του. Έτσι, εάν ένας επιτιθέμενος αποκτήσει τουλάχιστον το 51%, της υπολογιστικής ισχύος του BN, μπορεί να ελέγξει πλήρως το δίκτυο, καταργώντας τα πλεονεκτήματα του blockchain. Ιδιαίτερα ευάλωτα σε τέτοιες επιθέσεις είναι BNs που αποτελούνται από μικρό αριθμό κόμβων, ενώ σε πολύ μεγάλο δίκτυα, όπως το Bitcoin, είναι πρακτικά ανέφικτη.

Άλλες σημαντικές προκλήσεις, σχετιζόμενες με το blockchain, είναι η **μεγαλύτερη καθυστέρηση** σε σχέση με την κεντρική προσέγγιση (σε κάποιες περιπτώσεις) και η **διαρκώς αυξανόμενη αποθηκευμένη πληροφορία**. Αυτό οφείλεται στο γεγονός ότι το blockchain είναι μία αλυσίδα που διαρκώς επεκτείνεται, αφού δε διαγράφονται προηγούμενα blocks. Ακόμα η ενημέρωση του λογισμικού που «τρέχει» σε ένα BN, μπορεί να καταστεί ιδιαιτέρως πολύπλοκη. Αυτό διότι το σύνολο των κόμβων δεν ενημερώνεται την ίδια χρονική στιγμή, με αποτέλεσμα οι μη ενημερωμένοι κόμβοι να μη δέχονται τις συναλλαγές που δημιουργούν οι ενημερωμένοι, ως ορθές και έγκυρες και αντιστρόφως.

2.4 Κατηγορίες Συστημάτων Blockchain

Το blockchain αναπτύχθηκε ως ένα αμιγώς κατανεμημένο σύστημα βάσης δεδομένων, για την υποβοήθηση συναλλαγών με ψηφιακά νομίσματα. Ωστόσο με την ευρεία υιοθέτησή του από διαφόρων ειδών λογισμικά, κατέστη φανερό ότι συχνά η κεντρική εκτέλεση ορισμένων λειτουργιών ή ελέγχων αποδεικνύεται αποδοτικότερη και ασφαλέστερη. Αυτό όχι μόνο δεν αναιρεί, αλλά μάλλον ενισχύει τα οφέλη του blockchain για τις εφαρμογές αυτές. Έτσι τα τελευταία χρόνια σχεδιάζονται BNs που κατατάσσονται σε τρεις κατηγορίες, ανάλογα με το βαθμό και το είδος του κεντρικού ελέγχου που ασκείται σε αυτά: δημόσια, κοινοπραξίας και ιδιωτικά [15].

Σε μία **Δημόσια Αλυσίδα Κοινοπραξιών (Public Blockchain)** κάθε κόμβος, σε οποιοδήποτε σημείο του πλανήτη και αν βρίσκεται, διαθέτει πλήρη δικαιώματα στο σύστημα. Έχει λοιπόν πρόσβαση στην αποθηκευμένη πληροφορία, μπορεί να εκκινήσει συναλλαγές οι οποίες θα επικυρωθούν και θα εκτελεστούν, εφόσον είναι ορθές, αλλά και να συμμετέχει στην εξόρυξη και στην επίτευξη της ομοφωνίας. Η ασφάλεια των συναλλαγών, η μυστικότητα και η ακεραιότητα των δεδομένων βασίζονται αποκλειστικά στα crypto-economics, καθώς στη λειτουργία του συστήματος δεν εμπλέκεται καμία κεντρική οντότητα. Συνεπώς πρόκειται για ένα πλήρως κατανεμημένο δίκτυο.

Σε μία **Αλυσίδα Κοινοπραξιών Ομοσπονδίας (Consortium Blockchain)** το δικαίωμα συμμετοχής στην επίτευξη ομοφωνίας ανήκει σε μία μερίδα κόμβων (ομοσπονδία), οι οποίοι

συνήθως διακατέχονται από αμοιβαία εμπιστοσύνη. Κάθε συναλλαγή πρέπει να εγκριθεί από καθορισμένο ποσοστό των κόμβων της κοινοπραξίας ώστε να θεωρηθεί έγκυρη. Αρκετά τέτοια BNs επιτρέπουν την πρόσβαση στο ευρύ κοινό, παραχωρώντας τη δυνατότητα προσπέλασης των δεδομένων στον καθένα, ενώ άλλα περιορίζουν τη δυνατότητα αυτή σε συγκεκριμένους κόμβους. Ένα τέτοιο σύστημα μπορεί να χαρακτηριστεί ως μερικώς κατανεμημένο, καθώς ελέγχεται από ένα υποσύνολο των κόμβων του.

Σε μία **Ιδιωτική Αλυσίδα Κοινοπραξιών (Private Blockchain)** το δικαίωμα εισαγωγής, διαγραφής ή τροποποίησης των καταγραφών ανήκει αποκλειστικά σε έναν οργανισμό. Δικαιώματα συμμετοχής στο BN και προσπέλασης των δεδομένων μπορεί να διαθέτει είτε το ευρύ κοινό είτε ένας περιορισμένος αριθμός κόμβων. Πρόκειται δηλαδή για ένα σύστημα που ελέγχεται μέσω κεντρικής οντότητας, όπου η προσπέλαση των δεδομένων γίνεται με την αξιοποίηση κρυπτογραφικών μηχανισμών του blockchain.

Καθεμία από τις παραπάνω κατηγορίες παρουσιάζει διαφορετικά χαρακτηριστικά, πλεονεκτήματα και μειονεκτήματα με αποτέλεσμα να κρίνεται καταλληλότερη και αποδοτικότερη για διαφορετικές εφαρμογές. Στα πλεονεκτήματα των ιδιωτικών blockchain συγκαταλέγεται η δυνατότητα που δίνεται σε έναν οργανισμό να μεταβάλλει τους κανόνες και τις παραμέτρους των έξυπνων συμβολαίων, έτσι ώστε να έχει την αποκλειστική διαχείριση των συναλλαγών, πράγμα απαραίτητο σε αρκετές περιπτώσεις. Επιπλέον, με την ανάπτυξη blockchain ιδιωτικού ή ομοσπονδίας εξαλείφεται η πιθανότητα εκτέλεσης επιθέσεων πλειοψηφίας, στις οποίες είναι ιδιαίτερα ευάλωτα τα δημόσια BNs που περιλαμβάνουν μικρό αριθμό κόμβων. Οι συναλλαγές είναι φθηνότερες, διότι τις διαχειρίζεται περιορισμένος αριθμός κόμβων με σημαντική υπολογιστική ισχύ και όχι πλήθος κόμβων μικρής ισχύος. Λόγω της καλής συνεργασίας και αξιόπιστης διασύνδεσης μεταξύ των κόμβων της ομοσπονδίας, η καθυστέρηση περιορίζεται σημαντικά, ενώ επιτυγχάνεται και γρηγορότερη ανάκαμψη από σφάλματα.

Τα πλεονεκτήματα των δημόσιων blockchain προκύπτουν άμεσα από την ανάλυση που παρατίθεται στο υποκεφάλαιο 2.3.

Με τον συνδυασμό των τριών κατηγοριών συστημάτων blockchain μπορούν να προκύψουν και **υβριδικά συστήματα**. Τέτοια παραδείγματα είναι οι συναλλαγές μεταξύ δημόσιων και ιδιωτικών συστημάτων ή η ανάπτυξη έξυπνων συμβολαίων, που ελέγχονται από μοναδικό οργανισμό, σε ένα δημόσια blockchain.

2.5 Τομείς Αξιοποίησης Blockchain

Οι πρώτες πλατφόρμες η λειτουργία των οποίων βασίζεται στο blockchain, όπως το Bitcoin και το Ethereum, αφορούν κάποιας μορφής οικονομικές συναλλαγές. Από τη στιγμή της εμφάνισής τους η εξέλιξη των πληροφοριακών συστημάτων αυτών είναι διαρκής, όπως και η ανάπτυξη νέων, παρόμοιου σκοπού. Ωστόσο η δυναμική του blockchain, το οποίο έχει χαρακτηριστεί ως η τεχνολογία με τη μεγαλύτερη επίδραση στη ζωή των ανθρώπων κατά την τελευταία δεκαετία, δεν περιορίζεται σε αυτό [16]. Αντίθετα συντελούνται συστηματικές ερευνητικές προσπάθειες ενσωμάτωσής του σε ένα ευρύ φάσμα λογισμικών. Ενδεικτικές κατηγορίες αποτελούν οι εφαρμογές που αφορούν την υγεία [17], τη διαχείριση της εφοδιαστικής αλυσίδας [18], τη διαχείριση του εμπορίου ηλεκτρικής (και όχι μόνο) ενέργειας [19] και τα ασύρματα τηλεπικοινωνιακά συστήματα [3].

Πλήθος πληροφοριακών συστημάτων βρίσκουν εφαρμογή στο χώρο της υγείας, τα οποία συχνά διαχειρίζονται «ευαίσθητα» δεδομένα που σχετίζονται με την κατάσταση της υγείας του ασθενούς, τη συνταγογράφηση ή αφορούν σε κλινικές δοκιμές. Η ενσωμάτωση του blockchain σε τέτοια συστήματα αποσκοπεί στην διασφάλιση της μυστικότητας και της ακεραιότητας των δεδομένων αυτών. Κατά συνέπεια, διευκολύνεται σημαντικά η διαχείρισή τους, μια και καθίσταται εφικτός ο ασφαλής διαμοιρασμός τους μεταξύ των εμπλεκόμενων μερών (π.χ. μεταξύ ενός ασθενούς, των γιατρών που τον παρακολουθούν και του φαρμακοποιού που θα εκτελέσει την ιατρική συνταγή).

Η παγκοσμιοποίηση, ο διεθνής ανταγωνισμός, η συμπεριφορά των καταναλωτών και οι ποικίλες ρυθμιστικές διατάξεις καθιστούν ιδιαίτερα πολύπλοκη τη διαχείριση της εφοδιαστικής αλυσίδας. Προκειμένου να εξασφαλιστεί η βιωσιμότητα της διαδικασίας, απαιτείται η επιβεβαίωση ότι τα προϊόντα και οι διαδικασίες πληρούν συγκεκριμένα κριτήρια. Άλλες σημαντικές απαιτήσεις είναι η διαφάνεια των διαδικασιών και η εξασφάλιση της ιχνηλασιμότητας εντός της αλυσίδας (π.χ. κατά τις ανακλήσεις προϊόντων). Τα πληροφοριακά συστήματα που σχετίζονται με τη διαχείριση της εφοδιαστικής αλυσίδας ως επί το πλείστον είναι αυτόνομα, μη συμβατά μεταξύ τους και ελέγχονται κεντρικά, από μεμονωμένη εταιρία ή οργανισμό. Η ενσωμάτωση του blockchain αναμένεται να συμβάλει καθοριστικά στη συνεργασία τέτοιων συστημάτων και στην κάλυψη κενών ασφάλειας που είναι πιθανό να τα χαρακτηρίζουν, συμβάλλοντας στην καλύτερη διαχείριση αυτής της πολύπλοκης διαδικασίας.

Τις τελευταίες δεκαετίες, με την ευρεία εισαγωγή των Ανανεώσιμων Πηγών Ενέργειας στο ενεργειακό μείγμα δεν υπάρχει σαφής διαχωρισμός μεταξύ παραγωγής και κατανάλωσης σε ένα Σύστημα Ηλεκτρικής Ενέργειας. Η ανάπτυξη σχετικών πληροφοριακών συστημάτων που

ενσωματώνουν blockchain, παρέχοντας κατανεμημένη λειτουργία και υψηλό επίπεδο ασφάλειας πρόκειται να συμβάλλει καθοριστικά στην αντιμετώπιση πλήθους προβλημάτων, που αφορούν τη διαχείριση και την εποπτεία των πολύπλοκων αυτών συστημάτων. Έτσι διευκολύνεται το εμπόριο ενέργειας, με το συντονισμό της μεταφοράς μεταφορά της ισχύος από ένα σύστημα σε άλλο.

Πολλά υποσχόμενη μπορεί να χαρακτηριστεί και η ενσωμάτωση του blockchain στα ασύρματα τηλεπικοινωνιακά συστήματα και στο IoT, καθιστώντας τις προαναφερόμενες εφαρμογές διαθέσιμες οπουδήποτε, αλλά και εισάγοντας ποικίλες νέες δυνατότητες. Το συγκεκριμένο ζήτημα αναλύεται διεξοδικά στη συνέχεια της παρούσας διπλωματικής εργασίας.

3 Ενσωμάτωση Blockchain στα Ασύρματα Τηλεπικοινωνιακά Συστήματα

Στο παρόν κεφάλαιο παρατίθενται τα βασικά χαρακτηριστικά των σύγχρονων κυψελωτών τηλεπικοινωνιακών συστημάτων και οι βασικότερες εξελίξεις που πρόκειται να συντελεστούν σε αυτά τα προσεχή έτη. Ακόμα αναφέρονται τα κίνητρα που οδήγησαν στην εξέταση της ενσωμάτωσης του blockchain σε αυτά. Εν συνεχεία, αναλύεται ο τρόπος και τα ποικίλα σημεία του δικτύου, όπου αυτή αναμένεται να λάβει χώρα, μέσω της ανασκόπησης της σχετικής βιβλιογραφίας. Ιδιαίτερη έμφαση δίνεται στην αρχιτεκτονική του B-RAN, καθώς αποτελεί αντικείμενο της παρούσας εργασίας.

3.1 Ασύρματα Τηλεπικοινωνιακά Συστήματα

Τα ασύρματα τηλεπικοινωνιακά συστήματα, από τη στιγμή της εμπορικής αξιοποίησής τους, γύρω στο 1980, παρουσιάζουν ραγδαία και αδιάκοπη εξέλιξη, η επιρροή της οποίας στην ανθρώπινη καθημερινότητα είναι ιδιαιτέρως αισθητή [20], [21]. Ανά δέκα περίπου χρόνια, εμφανίζεται μία νέα γενιά, που εισάγει πλήθος καινοτόμων τηλεπικοινωνιακών υπηρεσιών και βελτιώνει τις ήδη προσφερόμενες. Αυτό επιτυγχάνεται με την αύξηση του ρυθμού μετάδοσης δεδομένων, τη μείωση της καθυστέρησης και την εφαρμογή καινοτόμων τεχνικών ή τεχνολογιών. Αξίζει να σημειωθεί ότι τα χαρακτηριστικά κάθε γενιάς δεν παγιώνονται αμέσως μετά την προτυποποίησή τους, αντίθετα βελτιώνονται συνεχώς, πολλές φορές ακόμα και μετά την έλευση των συστημάτων της επόμενης γενιάς.

Πιο συγκεκριμένα, στις αρχές της δεκαετίας του 1980, εμφανίστηκαν τα Κυψελωτά Τηλεπικοινωνιακά Συστήματα Πρώτης Γενιάς (First Generation – 1G), τα οποία λειτουργούν αναλογικά και οι δυνατότητές τους περιορίζονται σχεδόν αποκλειστικά στη μετάδοση φωνής. Ακολούθησαν τα Κυψελωτά Τηλεπικοινωνιακά Συστήματα Δεύτερης Γενιάς (Second Generation – 2G), που είναι ψηφιακά και χαρακτηρίζονται από σημαντική βελτίωση της ποιότητας των υπηρεσιών φωνής, ενώ παρέχουν τη δυνατότητα ανταλλαγής σύντομων γραπτών μηνυμάτων (Short Messaging Service – SMS) μεταξύ των συνδρομητών. Η δομή και η λειτουργία τους βασίζεται σε ένα κοινό πρότυπο για τις περισσότερες χώρες του κόσμου, το Global Systems for Mobile Communications (GSM), η ύπαρξη του οποίου επέλυσε αρκετά προβλήματα. Η εξέλιξη συνεχίστηκε με τα αντίστοιχα συστήματα της Τρίτης Γενιάς (Third

Generation – 3G), που περιγράφονται από το πρότυπο Universal Mobile Telecommunications System (UMTS).

Σήμερα, στις αρχές της δεκαετίας του 2020, τα δίκτυα 4G λειτουργούν σχεδόν σε κάθε γωνιά του πλανήτη, ενώ έχει ήδη ξεκινήσει η εμπορευματοποίηση των Κυψελωτών Τηλεπικοινωνιακών Συστημάτων Πέμπτης Γενιάς (Fifth Generation – 5G). Το ίδιο και οι συστηματικές ερευνητικές προσπάθειες καθορισμού των χαρακτηριστικών των αντίστοιχων συστημάτων της Έκτης Γενιάς (Sixth Generation – 6G).

Ο όρος B5G αναφέρεται στα ασύρματα δίκτυα της πέμπτης γενιάς, αλλά και των αμέσως επόμενων, κατά κύριο λόγο στα 6G. Η ανάγκη εισαγωγής του προκύπτει, καθώς πολλές δυνατότητες που αποτελούν υποσχέσεις των 5G, στην πράξη πρόκειται να προσφερθούν από τα συστήματα των επόμενων γενεών, όταν οι τεχνολογίες και πρακτικές υλοποίησής τους καταστούν αρκετά ώριμες. Επίσης κάποιες δυνατότητες αναμένεται να εισαχθούν από τα 5G, αλλά να βελτιστοποιηθούν και να καταστούν ευρέως διαθέσιμες και αποδεκτές από τα 6G.

Τα 4G διέπονται από το πρότυπο Long Term Evolution (LTE) [22]. Πρόκειται για δίκτυα που βασίζονται εξ' ολοκλήρου στο Πρωτόκολλο του Διαδικτύου (Internet Protocol – IP) (all IP networks), οπότε επιτρέπουν την εκτέλεση διαδικτυακών εφαρμογών στις 4G UEs, οι δυνατότητες των οποίων στις μέρες μας, προσεγγίζουν αυτές ενός προσωπικού υπολογιστή. Το γεγονός αυτό, σε συνδυασμό με την αξιοσημείωτη βελτίωση αρκετών ήδη παρεχόμενων υπηρεσιών και τις προσιτές τιμές UEs και εφαρμογών, συντέλεσε στην αποδοχή των συστημάτων αυτών από το ευρύ καταναλωτικό κοινό. Επίσης ο συνδυασμός των συστημάτων αυτών με το IoT, έχει δημιουργήσει νέες ανάγκες, που καλούνται να ικανοποιήσουν τα B5G.

Τα 5G υπόσχονται εντυπωσιακές βελτιώσεις, με ρυθμό δεδομένων μεγαλύτερο των 10 Gbps, καθυστέρηση μικρότερη του 1 msec, πολύ μεγαλύτερη αξιοπιστία και ενεργειακή αποδοτικότητα του δικτύου, καθώς και σημαντικότατη αύξηση του αριθμού των ταυτόχρονα εξυπηρετούμενων τερματικών εντός καθορισμένης γεωγραφικής περιοχής. Βέβαια οι μεγαλύτερες προσδοκίες από τα συστήματα της γενιάς αυτής αφορούν την ευρεία ενσωμάτωση του IoT, που αποτελεί καθοριστικό βήμα για τη μετάβαση σε έναν ψηφιακό κόσμο. Λόγω του πλήθους και της ετερογένειας των UEs, όπως και των εφαρμογών που αιτούνται, το δίκτυο πρέπει να προσαρμόζεται γρήγορα και αυτόματα στις απαιτήσεις της εκάστοτε εφαρμογής. Προκύπτουν έτσι τρεις κατηγορίες υπηρεσιών, ανάλογα με τις απαιτήσεις τους [23]:

- **Enhanced Mobile Broadband (eMBB)**: Αφορά την παροχή υπηρεσιών που σχετίζονται με την επικοινωνία μεταξύ ανθρώπων. Λαμβάνεται ειδική μέριμνα για πολλές

περιπτώσεις χρήσης, συχνά με διαφορετικές απαιτήσεις, όπως η κάλυψη ευρείας περιοχής και η κάλυψη μικρής σε έκταση περιοχής όπου βρίσκεται τεράστιο πλήθος UEs (π.χ. γήπεδο).

- **Ultra-Reliable and Low Latency Communications (URLLC)**: Αφορά σε εφαρμογές που χαρακτηρίζονται από αυστηρές απαιτήσεις σε εύρος ζώνης, καθυστέρηση και διαθεσιμότητα. Τέτοιες είναι η πραγματοποίηση χειρουργικών επεμβάσεων από ρομπότ, οι έλεγχοι κατά την παραγωγική διαδικασία και τα αυτοκίνητα χωρίς οδηγό. Γίνεται εύκολα αντιληπτό ότι οι αστοχίες και τα σφάλματα των συγκεκριμένων εφαρμογών (critical services) ή του δικτύου, σε πολλές περιπτώσεις, συνεπάγονται επικίνδυνες καταστάσεις.
- **Massive machine type communications (mMTC)**: Αφορά κυρίως το IoT, όπου συνδέονται ταυτόχρονα πολλές ετερογενείς UEs, που κατά κανόνα δεν έχουν αυξημένες απαιτήσεις ως προς το ρυθμό δεδομένων και τη καθυστέρηση. Ωστόσο το κόστος των συσκευών αυτών πρέπει να διατηρείται χαμηλό και να λαμβάνεται μέριμνα για τη διάρκεια ζωής της μπαταρίας, καθώς σε αρκετές UEs δεν υπάρχει η δυνατότητα επαναφόρτισης ή αντικατάστασής της.

Προκειμένου να επιτευχθούν οι φιλόδοξοι στόχοι του 5G, είναι απαραίτητη η εισαγωγή αρκετών καινοτόμων τεχνικών και τεχνολογιών. Αξιοποιούνται λοιπόν νέες συχνότητες στις τηλεπικοινωνιακές μεταδόσεις, που ανήκουν στο φάσμα των μικροκυμάτων (3.3 - 4.2 GHz), καθώς και σε αυτό των χιλιοστομετρικών κυμάτων (millimetre Waves – mmWaves), οπότε διευρύνεται το διαθέσιμο φάσμα. Αυτό είναι απαραίτητο για την ικανοποίηση ευρυζωνικών εφαρμογών, ενώ διευκολύνει τη διαχείριση και επαναχρησιμοποίηση των διαθέσιμων συχνοτήτων, συμβάλλοντας καθοριστικά στην αύξηση της ρυθμοαπόδοσης του συστήματος. Επίσης, με την ευρεία χρήση συστοιχιών Κεραιών Πολλαπλής Εισόδου και Εξόδου (massive Multiple Input Multiple Output – mMIMO), η δέσμη του μεταδιδόμενου σήματος είναι περισσότερο κατευθυντική. Οπότε αυξάνεται η ενεργειακή απόδοση του συστήματος και καθίσταται δυνατή η χρήση της Πολυπλεξίας και Πολλαπλής Προσπέλασης Δέσμης (Beam Division Multiple Access – BDMA).

Για την αύξηση της υπολογιστικής ισχύος του δικτύου και τη διαθεσιμότητα των αποθηκευμένων δεδομένων οπουδήποτε και οποτεδήποτε αξιοποιούνται τα Υπολογιστικά Νέφη (Cloud Computing – CC), αλλά και η Υπολογιστική Παρυφής (Edge Computing – EC). Η τελευταία παρέχει επεξεργαστική ισχύ και αποθηκευτικό χώρο σε μικρή απόσταση από σχεδόν οποιαδήποτε UE. Επίσης υπάρχει η τάση αντικατάστασης εξειδικευμένου υλικού δικτυακού

εξοπλισμού από λογισμικό, οπότε μειώνεται σημαντικά το κόστος ανάπτυξης και λειτουργίας του κυψελωτού συστήματος, αυξάνεται η ευελιξία του και η παραμετροποίησή του καθίσταται ιδιαίτερα εύκολη. Προς την κατεύθυνση αυτή συμβάλλει ουσιαστικά η τεχνολογία των Δικτύων Καθαρισμένων από Λογισμικό (Software Defined Network – SDN) [24], όταν συνδυάζεται με την Εικονοποίηση των Λειτουργιών Δικτύωσης (Network Function Virtualization – NFV) [25]. Σημαντική απαίτηση αποτελεί η προσαρμογή του δικτύου στις ιδιαιτερότητες της εκάστοτε εφαρμογής, πράγμα που επιτυγχάνει ο Τεμαχισμός του Δικτύου (Network Slicing – NS), προσφέροντας ένα κατάλληλα παραμετροποιημένο εικονικό δίκτυο. Πλήθος τέτοιων δικτύων εκτελούνται ταυτόχρονα από το ίδιο υλικό (υπολογιστικές μηχανές), ως εικονικές μηχανές.

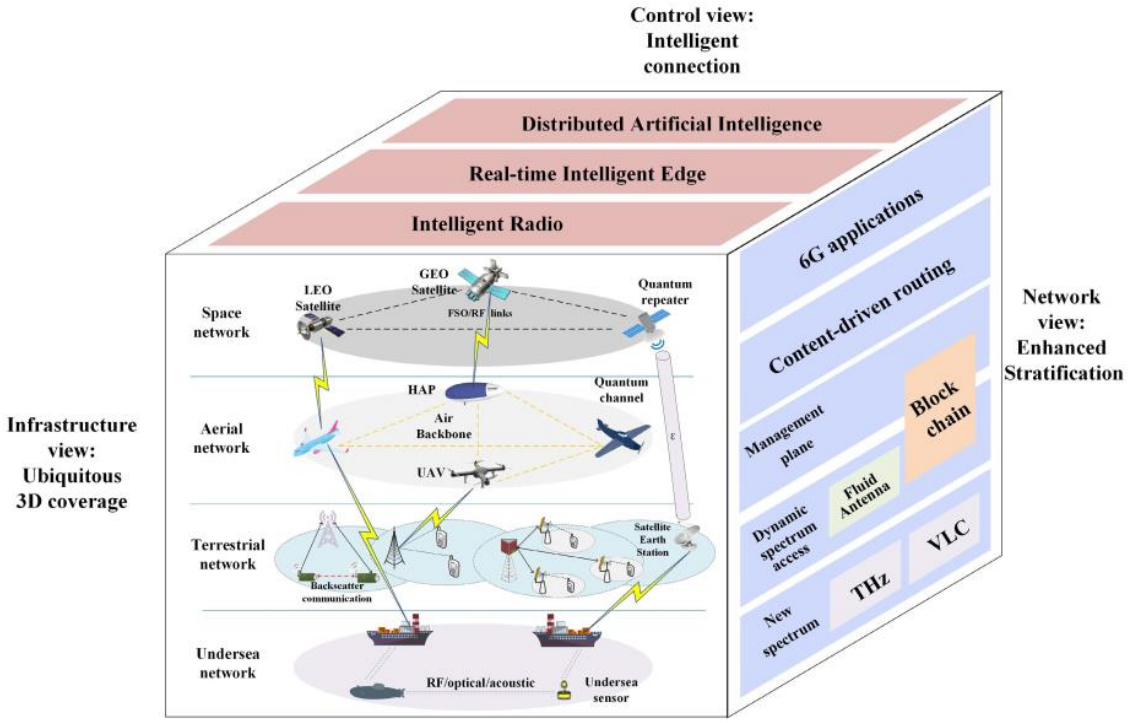
Την έναρξη της εμπορικής διάθεσης των 5G ακολούθησαν οι ερευνητικές δραστηριότητες που σχετίζονται με τα 6G [21], [26]. Κατ' αντιστοιχία με τα συστήματα κάθε επόμενης γενιάς, αυτά αναμένεται να προσφέρουν εντυπωσιακή βελτίωση του ρυθμού δεδομένων, της καθυστέρησης, της Ποιότητας της Υπηρεσίας (Quality of Service – QoS), αλλά και της Ποιότητας της Εμπειρίας (Quality of Experience – QoE), που πλέον συγκαταλέγεται στις μετρικές επίδοσης του δικτύου. Ωστόσο, η πραγματική επανάσταση των συστημάτων της γενιάς αυτής πρόκειται να επέλθει από την υψηλή ενεργειακή αποδοτικότητα του δικτύου, την προσθήκη ευφυΐας σε αυτό, την πανταχού (και αξιόπιστη) συνδεσιμότητα και την εξέλιξη του IoT στο Διαδίκτυο των Πάντων (Internet of Everything – IoE).

Για την επίτευξη των παραπάνω στόχων, η αρχιτεκτονική του δικτύου αναμένεται να μεταβληθεί γύρω από τρεις άξονες (Εικόνα 3-1):

- **Υποδομή:** Τα υπάρχοντα επίγεια ασύρματα τηλεπικοινωνιακά συστήματα πρόκειται να συνδυαστούν με άλλα, δορυφορικά, εναέρια και υποθαλάσσια, ώστε οι τηλεπικοινωνιακές υπηρεσίες να καταστούν διαθέσιμες οπουδήποτε και οποτεδήποτε είναι πιθανό να απαιτηθούν. Αυτό αποτελεί προϋπόθεση υλοποίησης του IoE, του οποίου ο ρόλος θα είναι καθοριστικός για τις έξυπνες πόλεις, τα έξυπνα σπίτια, την τηλεϊατρική και ρομποτική ιατρική, τα αυτο-οδηγούμενα αυτοκίνητα και πολλές άλλες καινοτόμες και ανατρεπτικές εφαρμογές.
- **Έλεγχος:** Η Τεχνητή Νοημοσύνη (Artificial Intelligence – AI) και ιδιαίτερα η Μηχανική Μάθηση (Machine Learning – ML), σχεδιάζεται να ενσωματωθεί σε ποικίλα σημεία του 6G, ώστε αυτό να ελέγχεται αυτόματα και αποδοτικά, αλλά και να παρέχεται «ευφυής» σύνδεση. Πιο συγκεκριμένα, προτείνεται η αξιοποίηση της AI για την αλληλεπίδραση μίας έξυπνης συσκευής με το περιβάλλον της σε πραγματικό χρόνο, τη δυναμική

προσαρμογή των αλγορίθμων που εκτελούνται στους πομποδέκτες στις τρέχουσες απαιτήσεις (π.χ. του υλικού) και την παράλληλη και κατανεμημένη λήψη αποφάσεων.

- **Στοίβα δικτυακού πρωτοκόλλου:** Το πρωτόκολλο TCP/IP έχει λειτουργήσει αποτελεσματικά και με ελάχιστες τροποποιήσεις, για αρκετά χρόνια. Ωστόσο τα πακέτα του επιπέδου δικτύου, ακολουθούν μία προκαθορισμένη δομή, αποτελούμενη από μία επικεφαλίδα και τα μεταφερόμενα δεδομένα, πράγμα που υποβαθμίζει την ικανότητα προσαρμογής του δικτύου στις απαιτήσεις της εκάστοτε εφαρμογής. Ανάλογη είναι και η κατάσταση του επιπέδου μεταφοράς. Έτσι εξετάζεται ο ανασχεδιασμός του IP, ώστε να επιτρέπει τον καθορισμό παραμέτρων από τον σχεδιαστή κάθε εφαρμογής, στοχεύοντας στην κατάλληλη προσαρμογή του δικτύου στις εκάστοτε απαιτήσεις.



Εικόνα 3-1 [26]: Σημαντικότερες πτυχές της αρχιτεκτονικής των 6G

Πολλά υποσχόμενη εμφανίζεται η πρόσβαση στο 6G εντός εσωτερικού χώρου, με την εκμετάλλευση των οπτικών συχνοτήτων, οι οποίες σε αντίθεση με τις ραδιοσυχνότητες, δεν χρησιμοποιούνται από άλλες εφαρμογές και είναι ευρέως διαθέσιμες. Έτσι διευκολύνεται σημαντικά η διαχείριση του φάσματος και αυξάνεται το φάσμα που διατίθεται για τις επικοινωνίες σε εξωτερικό χώρο. Η απόσταση μεταξύ Σημείου Πρόσβασης (Access Point – AP)

και UE σε εσωτερικό χώρο είναι συνήθως μικρή, πράγμα που συνεπάγεται την αύξηση της ενεργειακής απόδοσης με τη χρήση των οπτικών συχνοτήτων.

Μία ακόμα απαίτηση που πιθανότατα θα ικανοποιήσουν τα 6G είναι η μεγάλη αύξηση της αυτονομίας της μπαταρίας των UEs. Προς την κατεύθυνση αυτή, εξετάζεται η ασύρματη μεταφορά ενέργειας για τη φόρτιση της μπαταρίας, η εκμετάλλευση της ηλιακής ή άλλων ανεξάντλητων μορφών ενέργειας, για τον ίδιο σκοπό και ο περιορισμός των ενεργειακών απαιτήσεων αρκετών κατηγοριών UE. Οι προσδοκίες από το συνδυασμό των τεχνικών αυτών είναι ιδιαίτερα υψηλές.

Επιπλέον, γίνονται προσπάθειες συμμετοχής περισσότερων αισθήσεων των συνδρομητών στην εμπειρία που αποκομίζουν από τη χρήση των παρεχόμενων υπηρεσιών.

3.2 Κίνητρο Ενσωμάτωσης Blockchain σε B5G

Η αύξηση του πλήθους και η βελτίωση της ποιότητας των προσφερόμενων υπηρεσιών, που όπως φάνηκε πραγματοποιείται με τη μετάβαση σε κάθε επόμενη γενιά, συνοδεύεται από ταυτόχρονη αύξηση της πολυπλοκότητας των ασύρματων τηλεπικοινωνιακών συστημάτων και των σχετικών ζητημάτων που χρήζουν επίλυσης. Έτσι η επιστημονική κοινότητα αντιμετωπίζει ολοένα και μεγαλύτερες προκλήσεις στη σχεδίαση και την εμπορική υλοποίηση κυψελωτών δικτύων που να ανταποκρίνονται στις νέες ανάγκες που διαρκώς εμφανίζονται.

Σε ότι αφορά τα B5G ασύρματα δίκτυα, μία από τις κυριότερες προκλήσεις είναι η εγγύηση της ασφάλειας, της μυστικότητας και της ακεραιότητας των δεδομένων που αποθηκεύονται σε οντότητες του συστήματος ή ανταλλάσσονται κατά τη μεταξύ τους επικοινωνία. Τη λύση στο πρόβλημα, ή καθοριστικό μέρος αυτής, αναμένεται να δώσει η ενσωμάτωση του blockchain σε αρκετά σημεία των τηλεπικοινωνιακών συστημάτων αυτών.

Τα B5G αποτελούνται χονδρικά από δύο επιμέρους τμήματα, το RAN και το Δίκτυο Κορμού (Core Network – CN). Το πρώτο είναι υπεύθυνο για την εκτέλεση της διαδικασίας σύνδεσης κάθε UE στο δίκτυο, ενώ το CN είναι το κυρίως τηλεπικοινωνιακό δίκτυο, που διασυνδέει πλήθος RANs τόσο μεταξύ τους όσο και με άλλα ετερογενή δίκτυα, αποσκοπώντας στην παροχή της υπηρεσίας που αιτείται ο εκάστοτε συνδρομητής. Έτσι εξετάζοντας και πάλι το RAN, γίνεται κατανοητό ότι πρόκειται για το τμήμα του τηλεπικοινωνιακού συστήματος που παρεμβάλλεται μεταξύ οποιασδήποτε UE και του CN.

Η ενσωμάτωση του blockchain αναμένεται να λάβει χώρα τόσο στο RAN, όσο και στο CN. Για την επίτευξη μίας συγκεκριμένης διαδικασίας ή λειτουργίας του συστήματος, η διάκριση αυτή δεν είναι πάντοτε σαφής. Η παρούσα διπλωματική εργασία πραγματεύεται την ενσωμάτωση του blockchain στο RAN, οπότε δίνεται ιδιαίτερη έμφαση σε αυτή.

3.3 Βιβλιογραφική Ανασκόπηση

Την παρούσα χρονική στιγμή, η ενσωμάτωση του blockchain στα B5G βρίσκεται σε αρκετά πρώιμο στάδιο. Ωστόσο τα τελευταία χρόνια διεξάγονται συστηματικές ερευνητικές προσπάθειες, με τη σχετική διεθνή βιβλιογραφία να εμπλουτίζεται με γρήγορους ρυθμούς, καθώς πρόκειται για ένα πολλά υποσχόμενο ερευνητικό ζήτημα.

Διαφαίνεται ότι το blockchain μπορεί να συνεργαστεί αποτελεσματικά με τις βασικότερες τεχνολογίες που συνδυάζονται ώστε να υλοποιηθεί ένα B5G δίκτυο, όπως οι SDN, NFV, NS, CC/EC και επικοινωνία μεταξύ ομότιμων συσκευών (Device to Device – D2D) [3]. Σε αδρές γραμμές ο ρόλος του blockchain έγκειται στην εγγύηση της ασφάλειας, της μυστικότητας και της ακεραιότητας των αποθηκευμένων ή ανταλλασσόμενων δεδομένων, τόσο για τις κεντρικοποιημένες όσο και για τις κατανεμημένες τεχνολογίες. Στην πρώτη περίπτωση, συμβάλλει στη βιωσιμότητα μιας κατανεμημένης προσέγγισής τους, που συχνά αποτελεί απαίτηση των σύγχρονων συστημάτων, ενώ στη δεύτερη εισάγει ή ενισχύει τις ιδιότητες αυτές. Έτσι το blockchain διευκολύνει και βελτιστοποιεί πλήθος απαραίτητων διαδικασιών που λαμβάνουν χώρα στο δίκτυο, πράγμα που δίνει ώθηση στην ανάδυση αρκετών καινοτόμων εφαρμογών, που βαθμιαία μεταβάλλουν την ανθρώπινη καθημερινότητα [27].

Σε ότι αφορά τον ανασχεδιασμό του RAN των B5G δικτύων, συνεχώς κερδίζει έδαφος η ιδέα της ενσωμάτωσης του blockchain στη νέα αρχιτεκτονική του, η οποία αρχικά προτάθηκε στην επιστημονική δημοσίευση [4] και ονομάστηκε B-RAN. Στην ίδια εργασία παρουσιάζεται ένα πρωτόκολλο πρόσβασης στο δίκτυο αυτό και προτείνεται η αξιοποίηση του αλγόριθμου επίτευξης ομοφωνίας PoD, σε αντικατάσταση του PoW, πράγμα που υπόσχεται την ουσιαστική μείωση της καθυστέρησης και της κατανάλωσης ενέργειας. Βέβαια, αναλύονται και αρκετές προκλήσεις, η αντιμετώπιση των οποίων κρίνεται ζωτικής σημασίας για την ανάπτυξη της ιδέας αυτής στην πράξη.

Το blockchain δεν συνδυάζεται απλώς με τις βασικές τεχνολογίες του RAN, αλλά αποτελεί κεντρικό πυλώνα και δομικό στοιχείο της νέας προτεινόμενης αρχιτεκτονικής του. Στο πλαίσιο αυτό εξετάζεται ο ιεραρχικός διαχωρισμός των λειτουργιών του B-RAN σε έξι επίπεδα,

προκειμένου να κτιστεί η εμπιστοσύνη από το κατώτερο έως το ανώτερο επίπεδο του δικτύου [28].

Με τον τρόπο αυτό εκτός από την εκμετάλλευση των πλεονεκτικών χαρακτηριστικών του blockchain από το RAN (κατανεμημένη εγγύηση ασφάλειας και ακεραιότητας δεδομένων, χωρίς τη μεσολάβηση τρίτης οντότητας), προκύπτουν και άλλα, κυρίως οικονομικής φύσης πλεονεκτήματα. Δηλαδή καθώς το B-RAN επεκτείνεται, με τη συνένωση και άλλων επιμέρους RANs σε ένα ενιαίο, κατανεμημένο και αυτοελεγχόμενο δίκτυο, αυξάνεται το οικονομικό όφελος τόσο για τους παρόχους όσο και για τους συνδρομητές. Το χαρακτηριστικό αυτό καλείται «θετικές επιδράσεις δικτύου» (positive network effects) [28].

Ένα από τα πρώτα στάδια της μελέτης μιας νέας δικτυακής αρχιτεκτονικής είναι η ανάπτυξη προσομοιώσεων και πειραματικών διατάξεων (prototypes), με τις οποίες επιχειρείται η απόδειξη της δυνατότητας πρακτικής υλοποίησής της και η αποτίμηση των επιδόσεών που επιτυγχάνει. Συγκεκριμένα για το B-RAN, αρχικές τέτοιες προσπάθειες παρατίθενται στις δημοσιεύσεις [4], [28], απ’ όπου γίνεται κατανοητό ότι η ιδέα δύναται να λειτουργήσει στον πραγματικό κόσμο και μάλιστα παρουσιάζει αρκετά πλεονεκτήματα, συγκρινόμενη με τις «παραδοσιακές» προσεγγίσεις.

Στην [29] αναπτύχθηκε ένα prototype, που λαμβάνει υπόψη σαφώς μεγαλύτερο πλήθος παραμέτρων, συγκριτικά με τις προηγούμενες περιπτώσεις και αποσκοπεί στη μίμηση και την επίδειξη της λειτουργίας του B-RAN. Κατά τη διαδικασία της ανάπτυξης, αναδείχθηκαν και αντιμετωπίστηκαν αρκετά προβλήματα υλοποίησης της συγκεκριμένης τοπολογίας, όπως η αυξημένη καθυστέρηση πρόσβασης, οπότε εισήχθη ένας καινοτόμος και ταχύς μηχανισμός δημιουργίας και διαχείρισης των έξυπνων συμβολαίων, που ονομάστηκε Γρήγορη Ανάπτυξη Έξυπνων Συμβολαίων (Fast Smart Contract Deployment – FSCD). Προτείνεται επίσης η διαίρεση και η ψηφιοποίηση των διαθέσιμων πόρων φάσματος, προκειμένου να διευκολυνθεί ο αυτόματος διαμοιρασμός και συντονισμός τους σε ολόκληρο το δίκτυο.

Ως επέκταση της παραπάνω έρευνας, οι ίδιοι συγγραφείς όρισαν με σαφήνεια τη δομή του B-RAN και τα βήματα του πρωτοκόλλου πρόσβασης σε αυτό. Έπειτα το περιέγραψαν ως μία διαδικασία Markov, ομογενούς χρόνου, ξεκινώντας από την εξαγωγή ενός αναλυτικού μοντέλου περιγραφής της διαδικασίας γέννησης block. [30]. Μελέτησαν και περιέγραψαν αναλυτικά την καθυστέρηση, ενώ όρισαν τις μαθηματικές σχέσεις που διέπουν τις οριακές τιμές που αυτή μπορεί να λάβει. Επιπλέον μελετήθηκε το επίπεδο ασφάλειας του συστήματος, με κριτήριο την πιθανότητα εκτέλεσης επιτυχημένης επίθεσης, λαμβάνοντας υπόψη διαφορετικές στρατηγικές του επιτιθέμενου. Με την ανάλυση αυτή γίνεται αποτίμηση των παραγόντων υποβάθμισης της

ασφάλειας του συστήματος. Τέλος, επιβεβαιώθηκε η ορθότητα του συνόλου των εξαχθέντων αναλυτικών εκφράσεων, με τη βοήθεια του προηγούμενου prototype.

Η ενσωμάτωση του blockchain στα ασύρματα τηλεπικοινωνιακά συστήματα μπορεί να εξεταστεί και από τη σκοπιά των βασικών λειτουργιών ή διαδικασιών τις οποίες συνδράμει. Έτσι, η διεθνής βιβλιογραφία που αφορά το διαμοιρασμό του δικτυακού εξοπλισμού και του φάσματος, της υπολογιστικής αποφόρτισης (offloading), όπως και την τροποποίηση των χαρακτηριστικών του blockchain ώστε να εναρμονιστεί στις απαιτήσεις του IoT, μέρα με τη μέρα επεκτείνεται.

Όπως προαναφέρθηκε, στα B5G εμφανίζεται η πρόκληση της διαρκούς αύξησης του πλήθους και της ετερογένειας των UEs που καλείται να εξυπηρετήσει ταυτόχρονα το σύστημα. Προκειμένου να ανταπεξέλθει σε αυτές τις συνθήκες κάθε τηλεπικοινωνιακός πάροχος αναπτύσσει πλήθος μικροκυψελών (small cells) σε ολόκληρη την περιοχή όπου δραστηριοποιείται, πράγμα που αυξάνει σημαντικά το κόστος ανάπτυξης και λειτουργίας του δικτύου, το οποίο συχνά καθίσταται μη βιώσιμο. Τη λύση στο πρόβλημα δίνει η ιδέα της κοινής χρήσης του υλικού εξοπλισμού και των πόρων του δικτύου από πολλαπλούς παρόχους. Οι όροι του διαμοιρασμού καθορίζονται από τη Συμφωνία Επιπέδου Υπηρεσιών (Service Level Agreement – SLA) , που συνάπτεται μεταξύ των συνεργαζόμενων παρόχων.

Στο [31] προτείνεται η αυτόματη εκτέλεση SLAs, μεταξύ ιδιοκτητών μικροκυψελών και τηλεπικοινωνιακών παρόχων, ως έξυπνα συμβόλαια, οπότε εισάγεται η έννοια των μικροκυψελών ως Εφαρμογή (Small-Cell-as-a-Service – SCaaS). Αυτή παρέχει τη δυνατότητα σε κάθε ιδιώτη ή εταιρία να αποκτήσει δικαιώματα παροχής τηλεπικοινωνιακών υπηρεσιών.

Το ερευνητικό άρθρο [32] πραγματεύεται την ενσωμάτωση του blockchain στα σύγχρονα ασύρματα δίκτυα, ώστε να συνδράμει την αυτόματη σύναψη SLAs διαμοιρασμού μεταξύ των παρόχων, χωρίς τη μεσολάβηση κάποιας έμπιστης οντότητας. Συγκεκριμένα προτείνεται η ανάπτυξη ενός blockchain ομοσπονδίας στο CN, όπου μπορεί να μετέχει κάθε πάροχος, εφόσον το επιθυμεί. Επιπλέον η αποθήκευση των πληροφοριών ταυτοποίησης κάθε συνδρομητή στο blockchain, δύναται να αντικαταστήσει την οντότητα Home Subscriber Server (HSS), του LTE, διευκολύνοντας τη διαχείριση αρκετών πληροφοριών, αφού παραχωρείται το δικαίωμα προσπέλασής τους σε κάθε νόμιμα εμπλεκόμενη οντότητα.

Εκτός από την αξιοποίηση του blockchain κατά το διαμοιρασμό και τη διαχείριση του υλικού εξοπλισμού του δικτύου, αυτό μπορεί να συμβάλλει και στην αντίστοιχη διαδικασία που αφορά το διαθέσιμο φάσμα. Προς την κατεύθυνση αυτή κινείται η ερευνητική εργασία [33].

Παρά το γεγονός ότι πρόκειται για μια πρώιμη μελέτη, χωρίς ασφαλή συμπεράσματα, τα πλεονεκτήματα του blockchain στο πεδίο αυτό μοιάζουν αδιαμφισβήτητα. Αυτό είναι το γενικό συμπέρασμα που εξάγεται από τη διεξοδική διερεύνηση που διενεργείται σχετικά με τη συνδρομή και τον τρόπο ενσωμάτωσης του blockchain σε κάθε τύπο διαμοιρασμού ξεχωριστά. Με τον τρόπο αυτό εξασφαλίζεται η εναρμόνισή του με τις ιδιαιτερότητες του εκάστοτε τύπου. Διαφαίνεται πως η αξιοποίηση του blockchain κοινοπραξίας, αντί δημόσιου, συμβάλλει στην άμβλυνση αρκετών προβλημάτων. Επιπροσθέτως στο [34] προτείνεται ένα μοντέλο διαμοιρασμού του φάσματος, κατά τρόπο ώστε να περιορίζεται κατά το δυνατόν η υποχρησιμοποίησή του.

Μία ακόμα διαδικασία, την οποία πρόκειται να υποβοηθήσει το blockchain είναι το offloading. Για το σκοπό αυτό προτείνεται ο συνδυασμός του blockchain με το EC, ώστε να διασφαλιστεί η ακεραιότητα των ανταλλασσόμενων δεδομένων μεταξύ UEs και Κόμβων Παρυφής (Edge Nodes – ENs), χωρίς την ανάγκη μεσολάβησης κάποιας έμπιστης οντότητας [35]. Επίσης προτείνεται μία μέθοδος αυτόματης και βέλτιστης ισοκατανομής του υπολογιστικού φόρτου μεταξύ των ENs, που υπόσχεται την άμβλυνση αρκετών προβλημάτων που συνεπάγεται η άνιση κατανομή του υπολογιστικού φόρτου μεταξύ των ENs, όπως η καθυστέρηση και η πιθανότητα απώλειας δεδομένων. Από την εκτέλεση σχετικών προσομοιώσεων, γίνεται φανερό ότι αυτός ο στόχος εκπληρώνεται σε σημαντικό βαθμό.

Σε παραπλήσια κατεύθυνση κινείται και η δημοσίευση [36], όπου αναπτύσσεται μία καινοτόμος αρχιτεκτονική, βασιζόμενη στο blockchain, που αποσκοπεί στην ανάπτυξη μιας τοπολογίας υποστήριξης του offloading, αλλά και της περιαγωγής, τόσο στο περιβάλλον του διεθνούς B5G τηλεπικοινωνιακού συστήματος, όσο και στο σενάριο των Local 5G Operators (L5GOs). Μάλιστα το όφελος για τα δίκτυα L5GO πρόκειται να είναι μεγάλο, καθώς η πρακτική υλοποίηση των παραπάνω λειτουργιών σε αυτό, παρεμποδίζεται από ζητήματα μυστικότητας των δεδομένων, υψηλή καθυστέρηση, υψηλές αμοιβές οντοτήτων που δρουν ως μεσάζοντες και πιθανότητα απάτης. Η προτεινόμενη αρχιτεκτονική υπόσχεται να μετριάσει τα προαναφερόμενα προβλήματα, παρέχοντας δυναμική, αυτόματη και πραγματικού χρόνου περιαγωγή και offloading, με την εκμετάλλευση των πλεονεκτημάτων του blockchain.

Τα πιθανά οφέλη της ενσωμάτωσης του blockchain στα B5G είναι αρκετά και στην περίπτωση του IoT. Ωστόσο οι αντίστοιχες συσκευές συνήθως χαρακτηρίζονται από περιορισμένες υπολογιστικές ικανότητες και ενεργειακή αυτονομία. Οι περιορισμοί αυτοί έρχονται σε αντίθεση με τις απαιτήσεις της διατήρησης blockchain, καθώς ο υπολογισμός τιμών κατακερματισμού και γενικότερα η διαδικασία επίτευξης ομοφωνίας προϋποθέτει τόσο

σημαντικές υπολογιστικές δυνατότητες όσο και μεγάλη κατανάλωση ενέργειας. Έτσι, διεξάγονται ερευνητικές προσπάθειες προσαρμογής των χαρακτηριστικών του blockchain στις ιδιαιτερότητες του IoT.

Προτείνεται λοιπόν, ένα πρωτόκολλο πρόσβασης συσκευών IoT στο B-RAN, το Hash Access [37]. Υποστηρίζει μετάδοση χωρίς ανταλλαγή μηνυμάτων ελέγχου (grand-free), μια και ο όγκος των ανταλλασσόμενων δεδομένων είναι ως επί το πλείστον ιδιαίτερα μικρός. Η επιβολή της τήρησης των κανόνων προσπέλασης του κοινού μέσου, εξασφαλίζεται με τον υπολογισμό μίας τιμής κατακερματισμού, πριν την έναρξη της μετάδοσης. Προκύπτει από το μοναδικό αναγνωριστικό της συσκευής (ID), την τρέχουσα χρονική σφραγίδα και μία τιμή που εκπέμπει ευρέως (broadcast) το AP. Εάν η τιμή είναι μικρότερη ενός αριθμού – στόχου, που προσαρμόζεται στην εκάστοτε κατάσταση του δικτύου, η UE μεταδίδει αξιοποιώντας την τρέχουσα χρονοθυρίδα, διαφορετικά επιχειρεί σε επόμενη. Σε περίπτωση παράβασης του κανόνα από κάποια συσκευή, που γίνεται αντιληπτή από το AP μέσω της ανίχνευσης άκυρης τιμής, υπάρχει η δυνατότητα επιβολής κυρώσεων (προστίμου) στον αντίστοιχο συνδρομητή. Η χρήση του Διεθνούς Αναγνωριστικού Κινητού Εξοπλισμού (International Mobile Equipment Identity – IMEI), εκτός του ότι παραχαράσσεται δύσκολα, επιτρέπει μόνο μία προσπάθεια σε κάθε χρονοθυρίδα, οπότε αυξάνεται η ενεργειακή απόδοση. Ακόμα με το σχεδιασμό ενός καινοτόμου μηχανισμού πρόσβασης παρατηρείται σημαντική βελτίωση της καθυστέρησης, πράγμα που εξασφαλίζεται με την επικύρωση του αιτήματος και της πληρωμής αφού ξεκινήσει η εξυπηρέτηση του συνδρομητή.

Μία ακόμα παραπλήσια ιδέα αποτελεί η ενσωμάτωση του blockchain στο Νέφος των Πραγμάτων (Cloud of Things – CoT), οπότε προκύπτει το επονομαζόμενο Νέφος των Πραγμάτων βασιζόμενο σε Αλυσίδα Κοινοπραξιών (Blockchain Cloud of Things – BCoT) [38]. Με τον όρο CoT νοείται η αξιοποίηση του CC, ώστε να εκτελεστούν πολύπλοκοι υπολογισμοί και διαδικασίες σε αυτό, αντί στις IoT UEs. Όμως η κεντρικοποιημένη φύση του CC είναι σημαντικός παράγοντας περιορισμού των επιδόσεων του CoT, καθώς αποτελεί μοναδικό σημείο αστοχίας και δεν βοηθά στην επεκτασιμότητα του δικτύου. Επίσης η μεγάλη απόσταση του UE από τις υπολογιστικές μηχανές του CC αυξάνει την καθυστέρηση και την κατανάλωση ενέργειας, πράγμα απαγορευτικό για πολλές εφαρμογές. Οπότε το blockchain συμβάλλει στην αποκέντρωση αρκετών λειτουργιών του CoT, με την εγγύηση της ασφάλειας, μυστικότητας και ακεραιότητας των ανταλλασσόμενων δεδομένων που προσφέρει σε κάθε σύστημα που ενσωματώνεται. Δυνητικά, το BCoT θα συνδράμει στην εξέλιξη όλων σχεδόν των εισαγόμενων

εφαρμογών από τα B5G δίκτυα (έξυπνα σπίτια, πόλεις, βιομηχανία, εφαρμογές σχετιζόμενες με την υγεία, κ.α.).

Στη δημοσίευση [39] προτείνεται ο συνδυασμός του IoT με την Υπολογιστική Ομίχλης (Fog Computing), ώστε να συνδράμει στον έλεγχο του δικτύου, συντονίζοντας κατανεμημένα τους υπολογιστικούς και δικτυακούς πόρους. Επιπλέον σε UEs, που μεταδίδουν δεδομένα πολύ μικρού όγκου (Narrowband IoT – NB-IoT), ανατίθενται συγκεκριμένες χρονοθυρίδες μετάδοσης μικρού μήκους. Προκειμένου να ελαχιστοποιηθεί η ανταλλασσόμενη πληροφορία ελέγχου, σε τέτοιου είδους μεταδόσεις δεν ασκείται έλεγχος από το δίκτυο, πράγμα που συχνά οδηγεί σε συγκρούσεις [40]. Οπότε σύμφωνα με το προτεινόμενο πρωτόκολλο, κάθε φορά που μία NB-IoT συσκευή «επιθυμεί» να επιχειρήσει μετάδοση, εκκινεί μία συναλλαγή σε blockchain που μοιράζεται με άλλες παρόμοιες συσκευές που βρίσκονται στην ίδια περιοχή. Οι συγκρούσεις αποφεύγονται καθώς προτού μία συσκευή αξιοποιήσει μία χρονοθυρίδα ανατρέχει στο DL ώστε να ελέγξει εάν υπάρχουν προγραμματισμένες μεταδόσεις σε αυτή.

Τα χαρακτηριστικά του blockchain αποδεικνύονται ιδιαίτερα ελκυστικά και για το Βιομηχανικό Διαδίκτυο των Πραγμάτων (IIot – Industrial IoT). Ωστόσο οι περιορισμένες υπολογιστικές δυνατότητες και η μικρή ενεργειακή αυτονομία των IIoT UEs έρχονται σε αντίθεση με τις υψηλές επεξεργαστικές και ενεργειακές απαιτήσεις των συστημάτων blockchain που βασίζονται στον αλγόριθμο PoW ή παρόμοιους. Παρακινούμενοι από το πρόβλημα αυτό, οι συγγραφείς της ερευνητικής δημοσίευσης [41] προτείνουν μία «ελαφρύτερη» υλοποίηση ενός συστήματος blockchain, του LightChain, προσαρμοσμένη στις απαιτήσεις του IIot. Προτείνεται λοιπόν, ένας ενεργειακά αποδοτικός μηχανισμός επίτευξης ομοφωνίας, όπου η «δυσκολία» του mining ορίζεται δυναμικά, λαμβάνοντας υπόψη το φόρτο εργασίας των κόμβων. Ακόμα σχεδιάστηκε ένας νέος τρόπος διασποράς (broadcast), όπου δεν αποστέλλεται ολόκληρο το block, με αποτέλεσμα να περιορίζονται η αποστολή πλεονάζουσας πληροφορίας, συμβάλλοντας στη βελτίωση του ρυθμού δεδομένων που επιτυγχάνεται στο δίκτυο. Για τον περιορισμό του απαιτούμενου αποθηκευτικού χώρου στους κόμβους, προτείνεται μία μέθοδος επιλεκτικής αποθήκευσης πληροφορίας σε αυτούς, ενώ το υπόλοιπο τμήμα της να διατηρείται σε συστήματα μεγάλου αποθηκευτικού χώρου, ώστε να μην υποβαθμίζεται η ιχνηλασιμότητα των συναλλαγών. Η δυνατότητα πρακτικής υλοποίησης και η υπεροχή των προτεινόμενων διαδικασιών, συγκρινόμενες με τις «παραδοσιακές» προσεγγίσεις, επιβεβαιώνονται με την ανάπτυξη ενός κατάλληλου prototype.

4 Άμεση Πρόσβασης σε B-RAN

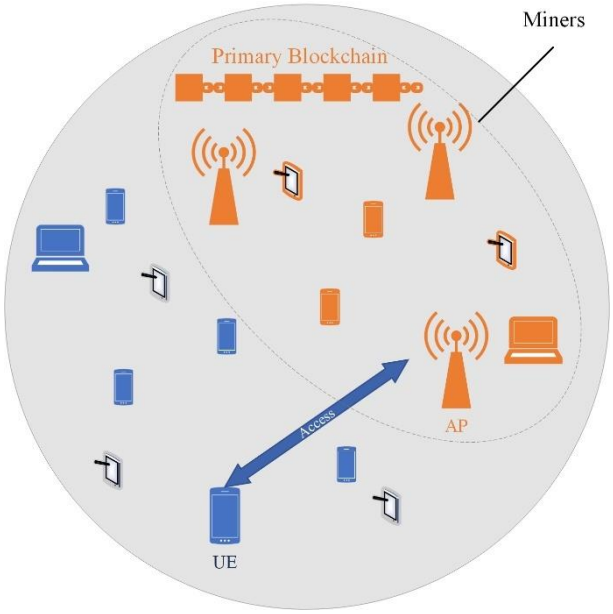
Το παρόν κεφάλαιο αφιερώνεται στη μελέτη του B-RAN, σύμφωνα με την αρχιτεκτονική που προτείνεται από τις ερευνητικές εργασίες [4] και [30]. Πιο συγκεκριμένα, παρουσιάζεται η τοπολογία του δικτύου και αναλύεται το πρωτόκολλο πρόσβασης σε αυτό. Στη συνέχεια το σύστημα μοντελοποιείται ως μία διαδικασία Markov ομογενούς χρόνου. Τέλος, διεξάγονται προσομοιώσεις προκειμένου να αποτιμηθούν οι επιδόσεις του B-RAN όσον αφορά την καθυστέρηση και την πιθανότητα αναμονής αιτήματος πρόσβασης σε ουρά, που υπερβαίνει δεδομένο αριθμό χρονικών μονάδων.

Ο κώδικας των προσομοιώσεων είναι διαθέσιμος στο GitHub [42].

4.1 Τοπολογία B-RAN και Πρωτόκολλο Πρόσβασης

Η απλούστερη προτεινόμενη τοπολογία του B-RAN παρουσιάζεται στην Εικόνα 4-1. Σύμφωνα με αυτή, το δίκτυο δομείται από συμβατικά APs, που διατηρούν περισσότεροι του ενός και συνεργαζόμενοι μεταξύ τους τηλεπικοινωνιακοί πάροχοι, καθώς και από μεγάλο πλήθος ετερογενών UEs. Η διεξαγωγή ασφαλούς και ιδιωτικής επικοινωνίας μεταξύ των συνεργαζόμενων παρόχων αποτελεί προϋπόθεση για τον έλεγχο και συντονισμό του δικτύου, αλλά και κατά τη σύνδεση οποιασδήποτε UE στο AP της επιλογής της. Για το σκοπό αυτό αναπτύσσεται και διατηρείται ένα blockchain από τους παρόχους. Έτσι σχηματίζεται ένα BN, όπου το δικαίωμα mining ανήκει στο σύνολο των εμπλεκόμενων παρόχων και προαιρετικά σε ορισμένους συνδρομητές που το επιθυμούν και είναι εφοδιασμένοι με «έξυπνες» συσκευές επαρκών υπολογιστικών δυνατοτήτων. Καθώς η επικουρική συμμετοχή ιδιωτών στο mining ή σε άλλες διαδικασίες που λαμβάνουν χώρα στο τηλεπικοινωνιακό σύστημα διευκολύνει σημαντικά τους παρόχους, συχνά αποφέρει προνόμια ως κίνητρα συμμετοχής.

Η διαδικασία αυτή αποσκοπεί στη δημιουργία ενός δικτύου πρόσβασης που οργανώνεται και ελέγχεται δυναμικά, κατανεμημένα και αυτόματα, δηλαδή αποτελεί ένα Αυτο-οργανούμενο Δίκτυο (Shelf Organized Network – SON). Αυτό προσαρμόζεται ταχύτατα στη στιγμιαία κατάστασή του, με στόχο την παροχή βέλτιστης QoS, την ελαχιστοποίηση του κόστους λειτουργίας του συστήματος και την κατά το δυνατόν αποδοτικότερη διαχείριση των πόρων του. Ο υψηλός βαθμός αυτοματοποίησης των λειτουργιών επιτυγχάνεται χάρη στα έξυπνα συμβόλαια. Με τον τρόπο αυτό, η ανθρώπινη παρέμβαση που απαιτείται για τη λειτουργία του δικτύου περιορίζεται στο ελάχιστο.



Εικόνα 4-1: Τοπολογία B-RAN

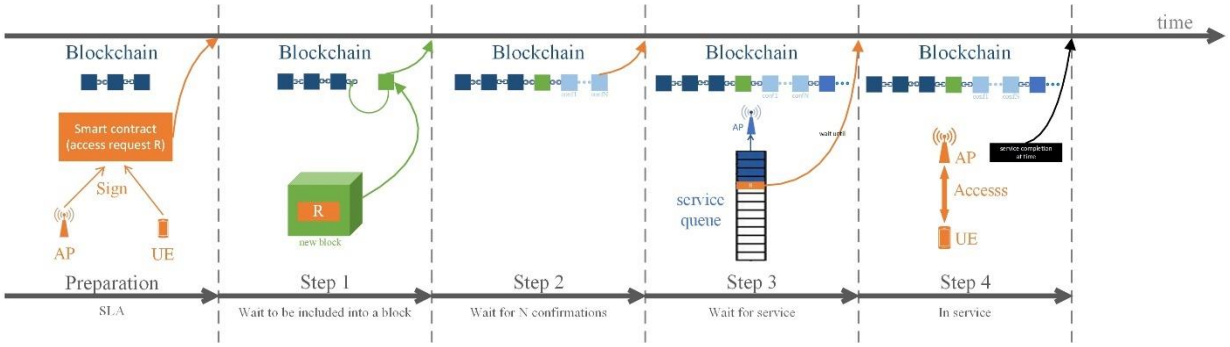
Προκειμένου ένας χρήστης να αποκτήσει πρόσβαση στο B-RAN, δηλαδή μία UE να συνδεθεί σε ένα AP, ακολουθείται ένα πρωτόκολλο αποτελούμενο από ένα προκαταρκτικό στάδιο και τέσσερα βήματα. Η χρονολογική εξέλιξη των γεγονότων παρουσιάζεται την Εικόνα 4-2. Πιο συγκεκριμένα:

- **Προκαταρκτικό στάδιο:** Μόλις μία UE υποβάλλει ένα αίτημα απόκτησης πρόσβασης στο B-RAN, γίνεται επίκληση σε ένα έξυπνο συμβόλαιο που ορίζει μία Συμφωνία Επιπέδου Υπηρεσίας (Service Level Agreement – SLA) μεταξύ παρόχου και συνδρομητή. Στο SLA προσδιορίζονται τα σημαντικότερα χαρακτηριστικά της παρεχόμενης σύνδεσης, όπως ο ρυθμός δεδομένων, η αμοιβή κ.α.

- **Βήμα 1:** Το έξυπνο συμβόλαιο, στο οποίο έχει καταγραφεί το αίτημα πρόσβασης, αποστέλλεται (broadcast) με τη μορφή συναλλαγής σε κάθε miner του δικτύου. Καθένας από αυτούς επιβεβαιώνει την ορθότητά της και την περιλαμβάνει στο υποψήφιο block που σχηματίζει, πιθανότατα μαζί με άλλες ομοειδείς συναλλαγές.

- **Βήμα 2:** Οι ορθές συναλλαγές περικλείονται στο υποψήφιο block που τελικά επικρατεί στο BN, το οποίο εν συνεχεία προσαρτάται στο τέλος της αλυσίδας. Τα αιτήματα που αντιστοιχούν στις συναλλαγές αυτές, αναμένουν την άφιξη ενός ελάχιστου καθορισμένου αριθμού (έστω N) νέων blocks, καθένα από τα οποία λογίζεται ως μία επιπλέον επιβεβαίωση.

- **Βήμα 3:** Αφού ένα αίτημα λάβει N επιβεβαιώσεις, θεωρείται επικυρωμένο και η πληροφορία του καταχωρείται στο DL. Εάν τη στιγμή που ένα αίτημα λαμβάνει την επιβεβαίωση με αριθμό N, το δίκτυο δεν έχει διαθέσιμο ασύρματο δίαυλο πρόσβασης, αυτό εισέρχεται σε μία ουρά αναμονής. Μόλις απελευθερωθεί κάποιος δίαυλος, ανατίθεται αυτός στο αίτημα που βρίσκεται στην πρώτη θέση της ουράς, που ακολουθείται η πολιτική Πρώτος Εντός Πρώτος Εκτός (First In First Out – FIFO).
- **Βήμα 4:** Η συσκευή έχει αποκτήσει πρόσβαση στο δίκτυο και η εξυπηρέτηση του συνδρομητή στον οποίο ανήκει διέπεται από τους όρους του SLA που διαμορφώθηκε κατά το προκαταρκτικό στάδιο.



Εικόνα 4-2: Βήματα πρωτοκόλλου πρόσβασης σε B-RAN

4.2 Μοντελοποίηση Άμεσης Πρόσβασης ως Διαδικασία Markov

Στο [30] αποδεικνύεται ότι οι αφίξεις αιτημάτων πρόσβασης στο B-RAN, είναι στατιστικά ανεξάρτητες και μπορούν να προσεγγιστούν ικανοποιητικά από την κατανομή Poisson. Εάν λ_a είναι ο μέσος ρυθμός αφίξεων αιτημάτων, ο χρόνος μεταξύ δύο διαδοχικών αφίξεων ακολουθεί την εκθετική κατανομή και έχει μέση τιμή:

$$\mu_a = \frac{1}{\lambda_a}$$

Τότε, βάσει μελετών [43], ο τυχαίος χρόνος τερματισμού της εξυπηρέτησης αιτημάτων θα ακολουθεί επίσης την εκθετική κατανομή, με μέση τιμή:

$$\mu_c = \frac{1}{\lambda_c}$$

όπου λ_c ο ρυθμός περάτωσης της εξυπηρέτησης αιτημάτων

Ακόμα, αποδεικνύεται ότι και η διαδικασία γέννησης blocks μπορεί να προσεγγιστεί ικανοποιητικά από την κατανομή Poisson (έστω ρυθμός αφίξεων blocks λ_b), δηλαδή ο χρόνος μεταξύ δύο διαδοχικών γεννήσεων blocks είναι εκθετικός, με μέση τιμή:

$$\mu_b = \frac{1}{\lambda_b}$$

Έτσι ο μέσος ρυθμός εμφάνισης γεγονότων (οποιουδήποτε είδους: άφιξη αιτήματος πρόσβασης, γέννηση block ή ολοκλήρωση εξυπηρέτησης αιτήματος) στο δίκτυο, βάσει των ιδιοτήτων της κατανομής Poisson, θα είναι:

$$\lambda = \lambda_a + \lambda_b + \lambda_c$$

Συνεπώς, ο μέσος χρόνος μεταξύ δύο διαδοχικών γεγονότων στο σύστημα είναι εκθετικός, με μέση τιμή:

$$\mu = \frac{1}{\lambda}$$

Σύμφωνα με τα βήματα του πρωτοκόλλου πρόσβασης, όπως παρουσιάζονται στο υποκεφάλαιο 4.1, το B-RAN μπορεί να μοντελοποιηθεί με τη βοήθεια της θεωρίας ουρών αναμονής. Οπότε η κατάσταση του συστήματος, μια τυχαία χρονική στιγμή t, μπορεί να περιγράφει από ένα διάνυσμα της μορφής:

$$X(t) = E(i_0, i_1, \dots, i_{N-1}, k)$$

Όπου:

i_n: ο αριθμός των αιτημάτων πρόσβασης που βρίσκονται στο δίκτυο και έχουν λάβει n επιβεβαιώσεις, έως τη χρονική στιγμή t

N: ο ελάχιστος αριθμός επιβεβαιώσεων που πρέπει να λάβει ένα αίτημα ώστε να θεωρηθεί επικυρωμένο

k: ο αριθμός των επικυρωμένων αιτημάτων πρόσβασης, δηλαδή με N ή περισσότερες επιβεβαιώσεις, που αναμένουν (στην ουρά) την απελευθέρωση καναλιού, ώστε να επιτευχθεί η πρόσβαση του αιτούμενου συνδρομητή στο δίκτυο.

Με μία πρώτη ματιά η μοντελοποίηση του B-RAN φαίνεται αρκετά πολύπλοκη, διότι είναι πιθανή η ταυτόχρονη επικύρωση πολλαπλών αιτημάτων, ο αριθμός των οποίων είναι διαφορετικός κάθε φορά. Ωστόσο παρατηρούμε ότι το μοντέλο μπορεί να αναχθεί σε μια διαδικασία Markov ομογενούς χρόνου, καθώς ισχύουν οι αντίστοιχες ιδιότητες:

Markov:

$$Pr\{X(t+h) = E|X(t) = E_i, X(u)\ for\ 0 \le u \le t\} = Pr\{X(t+h) = E|X(t) = E_i\}$$

Χρονική ομογένεια:

$$Pr\{X(t+h)E|X(t) = E_i\} = Pr\{X(t) = E|X(0) = E_i\}$$

όπου με E_i συμβολίζεται η κατάσταση του συστήματος τη χρονική στιγμή εκκίνησης της παρατήρησής του

Στην Εικόνα 4-3 φαίνεται το διάγραμμα μετάπτωσης καταστάσεων του B-RAN, όταν αυτό περιγράφεται από το διάνυσμα $X(t)$. Θεωρώντας μία τυχαία χρονική στιγμή, έστω t, ως στιγμή έναρξης της παρατήρησης του συστήματος το διάνυσμα αρχικής κατάστασης θα είναι:

$$X_i(t) = E_i(i_0, i_1, \dots, i_{N-1}, k)$$

Μετά τη διέλευση χρονικού διαστήματος h, επαρκώς μικρού ώστε να μπορεί να εμφανιστεί το πολύ ένα γεγονός κατά τη διάρκειά του, το σύστημα μεταβαίνει σε μία και μόνο μία από τις παρακάτω καταστάσεις:

- Με την **άφιξη ενός αιτήματος πρόσβασης**, τη χρονική στιγμή $(t+h)$ βρίσκεται στο σύστημα ένα επιπλέον αίτημα χωρίς καμία επιβεβαίωση, οπότε αυτό μεταβαίνει στην κατάσταση:

  $$X(t+h) = E(i_0 + 1, i_1, \dots, i_{N-1}, k)$$

  με πιθανότητα:

  $$Pr(A) = \lambda_a h$$

  Όπου: A το γεγονός άφιξης ενός αιτήματος πρόσβασης

- Με τη **γέννηση ενός block**, όλα τα αιτήματα που βρίσκονται στο σύστημα λαμβάνουν μία επιπλέον επιβεβαίωση, οπότε αυτό μεταβαίνει στην κατάσταση:

  $$X(t+h) = E(0, i_0, i_1, \dots, i_{N-1}, k)$$

  με πιθανότητα:

  $$Pr(B) = \lambda_b h$$

  Όπου: B το γεγονός γέννησης ενός block

- Με την **ολοκλήρωση της εξυπηρέτησης ενός αιτήματος**, απελευθερώνεται ένα κανάλι πρόσβασης το οποίο αμέσως ανατίθεται στο αίτημα που βρίσκεται στην πρώτη θέση της ουράς αναμονής, οπότε το σύστημα μεταβαίνει στην κατάσταση:

  $$X(t+h) = E(i_0, i_1, \dots, i_{N-1}, k-1)$$

  με πιθανότητα:

  $$Pr(C) = \lambda_c h$$

  όπου C το γεγονός της περάτωσης της εξυπηρέτησης ενός αιτήματος

  Να σημειωθεί ότι μπορεί να υπάρξει ολοκλήρωση της εξυπηρέτησης κάποιου αιτήματος αν και μόνο αν υπάρχει τουλάχιστον ένα τέτοιο στους εξυπηρετητές του συστήματος. Επίσης μετά την ολοκλήρωση εξυπηρέτησης αιτήματος, το κανάλι επικοινωνίας παραμένει ελεύθερο, στην περίπτωση που η ουρά αναμονής είναι κενή τη στιγμή t.

- Τέλος, μπορεί κατά το χρονικό διάστημα $(t+h)$ να μην εμφανιστεί **κανένα** από τα παραπάνω γεγονότα, οπότε το σύστημα παραμένει στην ίδια κατάσταση:

  $$X(t+h) = E_i(t)$$

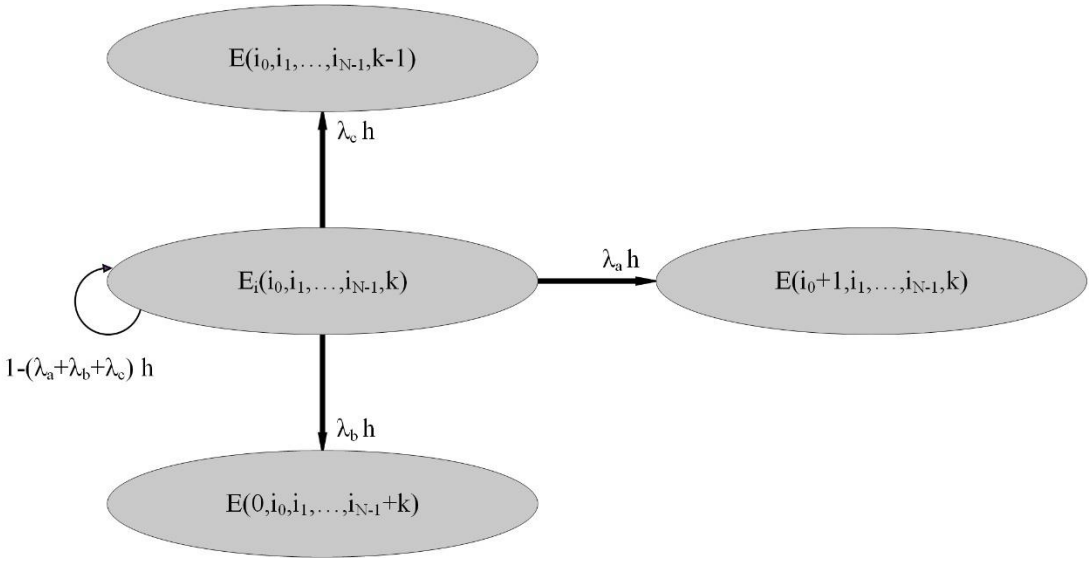
  με πιθανότητα:

  $$Pr(D) = 1 - (\lambda_a + \lambda_b + \lambda_c)h,$$

  Όπου: το D αντιστοιχεί στην περίπτωση κατά την οποία η κατάσταση του συστήματος παραμένει αμετάβλητη

  Δηλαδή πρόκειται για την πιθανότητα να μην εμφανιστεί κανένα από τα γεγονότα του δειγματικού χώρου.

Είναι χαρακτηριστικό το γεγονός πως για την περιγραφή των παραπάνω καταστάσεων αρκούν μόνο οι παράμετροι $\lambda_a, \lambda_b, \lambda_c, s, N$



Εικόνα 4-3: Διάγραμμα μετάπτωσης καταστάσεων B-RAN

4.3 Αποτελέσματα Προσομοιώσεων

Η παρούσα υπο-ενότητα αφορά την αξιολόγηση των επιδόσεων του B-RAN, με την ανάπτυξη προσομοιώσεων σε περιβάλλον MATLAB / Octave. Οι χρησιμοποιούμενοι Βασικοί Δείκτες Επίδοσης (Key Performance Indicators – KPIs) του δικτύου είναι η μέση καθυστέρηση (L) και η πιθανότητα αναμονής (p). Ως μέση καθυστέρηση ορίζεται το χρονικό διάστημα που μεσολαβεί από την άφιξη ενός αιτήματος πρόσβασης ως τη στιγμή που ανατίθεται ένα κανάλι πρόσβασης του δικτύου στην εξυπηρέτηση του συνδρομητή που υπέβαλλε το συγκεκριμένο αίτημα. Να σημειωθεί ότι στις προσομοιώσεις δεν λαμβάνεται υπόψη η καθυστέρηση διάδοσης block, καθώς είναι αρκετά μικρή για να επηρεάσει τα εξαγόμενα αποτελέσματα. Η πιθανότητα αναμονής αφορά την παραμονή αιτήματος σε ουρά για περισσότερες χρονικές μονάδες από ένα καθοριζόμενο κατώφλι. Εδώ εξετάζουμε τις περιπτώσεις όπου η αναμονή υπερβαίνει τη μία, τις δύο και τις τρεις χρονικές μονάδες.

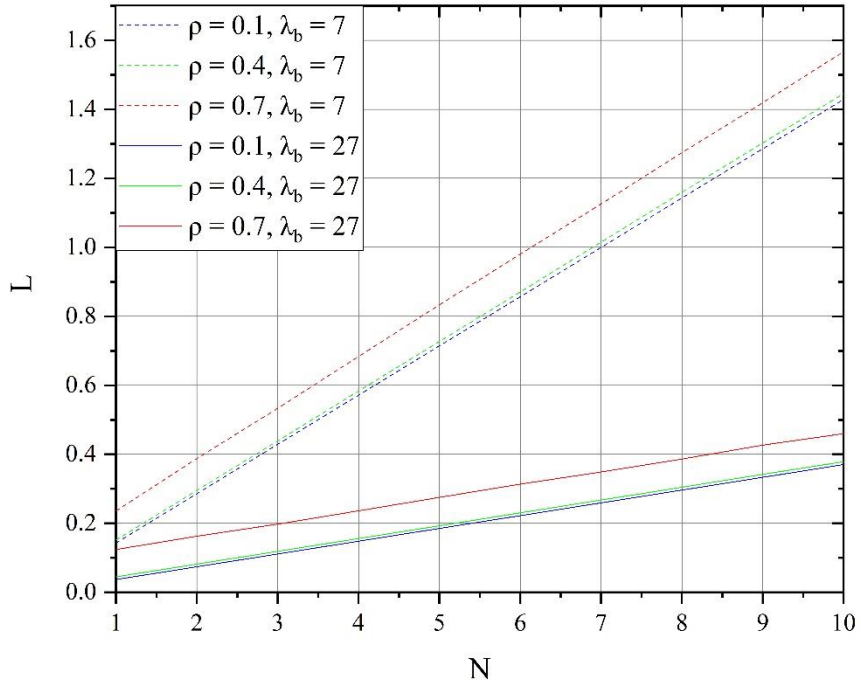
Για την εξαγωγή ασφαλών συμπερασμάτων, κρίνεται απαραίτητη η μελέτη των βασικών δεικτών επίδοσης για διαφορετικές τιμές της έντασης τηλεπικοινωνιακής κίνησης (ρ), η οποία ορίζεται ως εξής:

$$\rho = \frac{\lambda_a}{s\lambda_c}$$

όπου s ο αριθμός των διαθέσιμων καναλιών πρόσβασης του συστήματος. Εδώ, εξάγουμε αποτελέσματα για συνθήκες υψηλής, μέτριας και χαμηλής τηλεπικοινωνιακής κίνησης, με $\rho = 0.1$, $\rho = 0.4$ και $\rho = 0.7$, αντίστοιχα.

Κριτήριο τερματισμού κάθε προσομοίωσης αποτελεί η ολοκλήρωση της εξυπηρέτησης ενός εκατομμυρίου αιτημάτων πρόσβασης, ενώ ο ρυθμός περάτωσης της εξυπηρέτησης αιτημάτων τίθεται ίσος με τη μονάδα ($\lambda_c = 1$). Έτσι κάθε αποτέλεσμα που εξάγεται από τις προσομοιώσεις είναι εκφρασμένο στις μονάδες του χρόνου εξυπηρέτησης.

Με τη βοήθεια της πρώτης προσομοίωσης εξετάζεται η επίδραση του ελάχιστου αριθμού επιβεβαιώσεων για την επικύρωση ενός αιτήματος (N), όταν αυτός λαμβάνει τιμές από 1 έως 10, στη μέση καθυστέρηση (L), για χαμηλή, μέση και υψηλή τηλεπικοινωνιακή κίνηση. Ο αριθμός των διαθέσιμων καναλιών πρόσβασης του συστήματος λαμβάνεται ως $s = 5$, ενώ εξάγονται αποτελέσματα για ρυθμούς γέννησης blocks $\lambda_b = 7$ και $\lambda_b = 27$, τα οποία παρουσιάζονται στην Εικόνα 4-4.



Εικόνα 4-4: Μεταβολή καθυστέρησης (L) ως συνάρτηση του ελάχιστου αριθμού επιβεβαιώσεων (N), σε B-RAN

Από την προαναφερόμενη εικόνα, εξάγεται το συμπέρασμα ότι για δεδομένες τιμές των παραμέτρων ρ και λ_b, αύξηση της τιμής του N οδηγεί σε αύξηση της τιμής του L. Αυτό συμβαίνει διότι ένα αίτημα απαιτείται να αναμένει τη γέννηση περισσότερων blocks προκειμένου να θεωρηθεί επικυρωμένο και να καταστεί δυνατή η έναρξη της εξυπηρέτησής του. Παραδείγματος χάρη, για $\rho = 0.7$ και $\lambda_b = 7$, καθώς η τιμή του N αυξάνεται από το 3 έως το 8, το L αυξάνεται προοδευτικά από 0.43 σε 1.14.

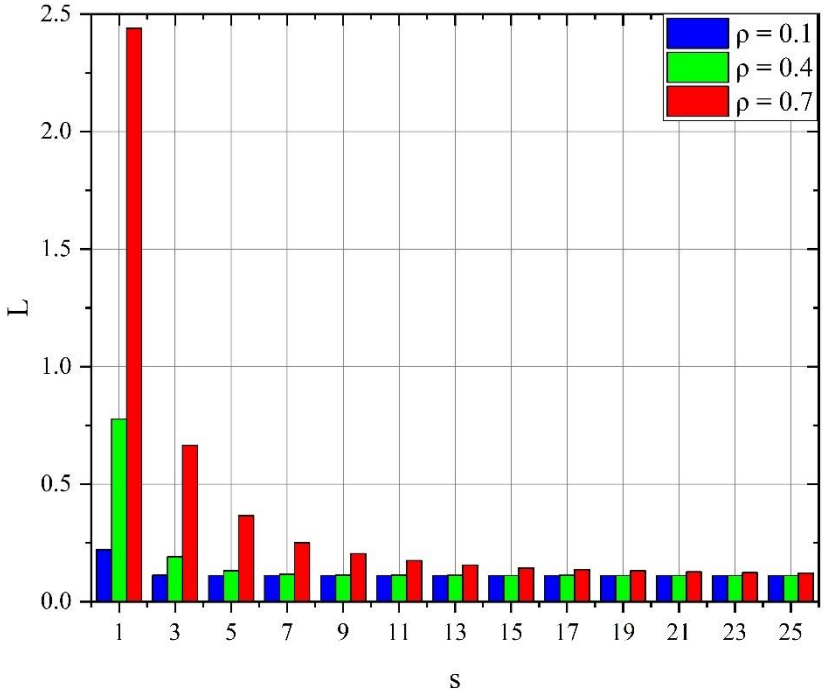
Επιπλέον διατηρώντας σταθερές τις παραμέτρους N και λ_b, γίνεται αντιληπτό ότι αυξάνοντας το ρ αυξάνεται και η L, καθώς όταν το δίκτυο λειτουργεί κάτω από υψηλότερη τηλεπικοινωνιακή κίνηση (μεγαλύτερος αριθμός αφίξεων αιτημάτων πρόσβασης ανά μονάδα χρόνου) τα διαθέσιμα κανάλια πρόσβασης εξαντλούνται συντομότερα, γεγονός που συνεπάγεται μεγαλύτερο χρόνο παραμονής των αιτημάτων στην ουρά. Θεωρώντας $N = 5$ και $\lambda_b = 27$, η τιμή του L είναι περίπου 0.185, για $\rho = 0.1$, ενώ αυξάνεται σε 0.193, για $\rho = 0.4$ και σε 0.275, για $\rho = 0.7$.

Μία ακόμα παρατήρηση έγκειται στο γεγονός ότι η αύξηση του λ_b, διατηρώντας σταθερές τις υπόλοιπες παραμέτρους, οδηγεί σε αρκετά μεγάλη μείωση της L, αφού ο μεγαλύτερος ρυθμός γέννησης blocks πρακτικά περιορίζει το χρόνο αναμονής των αιτημάτων μέχρι την επικύρωσή τους. Για παράδειγμα θεωρώντας $\rho = 0.4$, $N = 3$ και $\lambda_b = 27$ η καθυστέρηση είναι περίπου 0.439, όταν για $\lambda_b = 27$ μειώνεται σε μόλις 0.119 χρονικές μονάδες. Συνεπώς, η αύξηση του ρυθμού γέννησης blocks είναι ένας τρόπος μείωσης της καθυστέρησης. Αυτό όμως συμβαίνει μέχρι ενός σημείου, καθώς η υπέρμετρη αύξησή του δημιουργεί άλλα προβλήματα στο σύστημα.

Η δεύτερη προσομοίωση αποσκοπεί στον καθορισμό της σχέσης του αριθμού των διαθέσιμων καναλιών πρόσβασης του συστήματος (s) και της μέσης καθυστέρησης (L). Και αυτή η περίπτωση μελετάται για χαμηλή, μέτρια και υψηλή ένταση τηλεπικοινωνιακής κίνησης, ενώ στο s ανατίθενται τιμές από 1 έως 25, με ρυθμό αύξησης 2. Σε ότι αφορά τις υπόλοιπες παραμέτρους της προσομοίωσης, ο ρυθμός γέννησης blocks λαμβάνει την τιμή $\lambda_b = 27$ και ο ελάχιστος αριθμός επιβεβαιώσεων τίθεται ως $N = 3$.

Στην Εικόνα 4-5 παρουσιάζονται τα αποτελέσματα της παραπάνω προσομοίωσης. Εξάγεται το συμπέρασμα ότι με την αύξηση του s και διατηρώντας σταθερές τις υπόλοιπες παραμέτρους, μειώνεται η L, καθώς υπάρχουν περισσότερα διαθέσιμα κανάλια πρόσβασης στο τηλεπικοινωνιακό σύστημα. Οπότε ο αριθμός των αιτημάτων που εξυπηρετούνται την επόμενη χρονική στιγμή από την επικύρωσή τους (χωρίς να εισέλθουν στην ουρά) αυξάνεται, ενώ ο χρόνος αναμονής για τα αιτήματα που θα απαιτηθεί να εισέλθουν στην ουρά μειώνεται. Ως παράδειγμα, για $\rho = 0.1$, καθώς το s αυξάνεται από 1 σε 11, το L μειώνεται από 0.222 σε 0.111. Αυτή η μείωση παρατηρείται μέχρι μία τιμή – κατώφλι του s, που εξαρτάται από την ένταση της τηλεπικοινωνιακής κίνησης, πέραν της οποίας η L δεν ελαττώνεται περαιτέρω, διότι ο αριθμός – κατώφλι των καναλιών είναι αρκετός ώστε ελάχιστα αιτήματα να εισάγονται στην ουρά, για την υφιστάμενη τηλεπικοινωνιακή κίνηση. Μεγαλύτερη αύξηση των διαθέσιμων

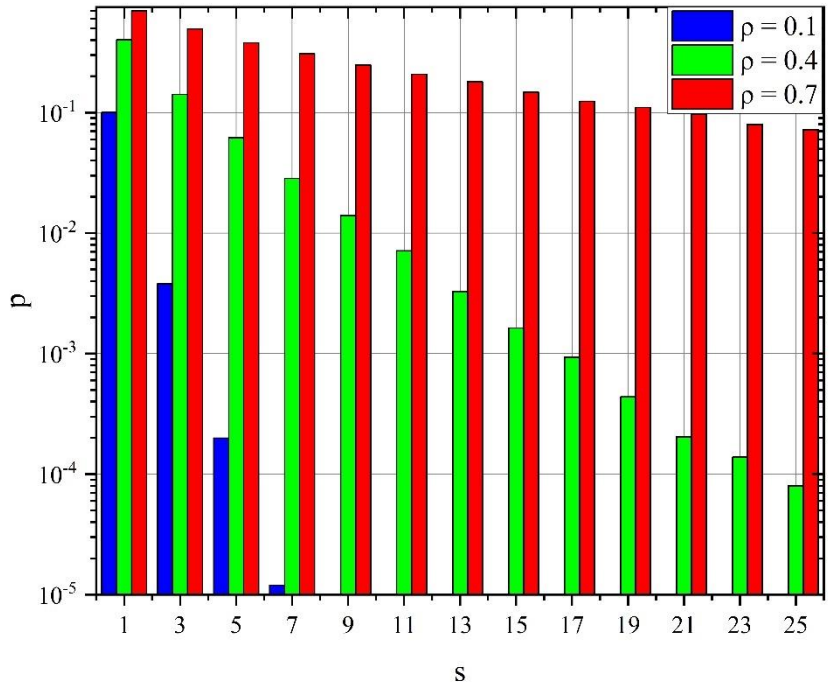
καναλιών δεν έχει κάποια σημαντική επίδραση στη μέση καθυστέρηση. Εδώ για χαμηλή και μέτρια ένταση, αυτό φαίνεται να επιτυγχάνεται για 7 και περισσότερα διαθέσιμα κανάλια πρόσβασης.



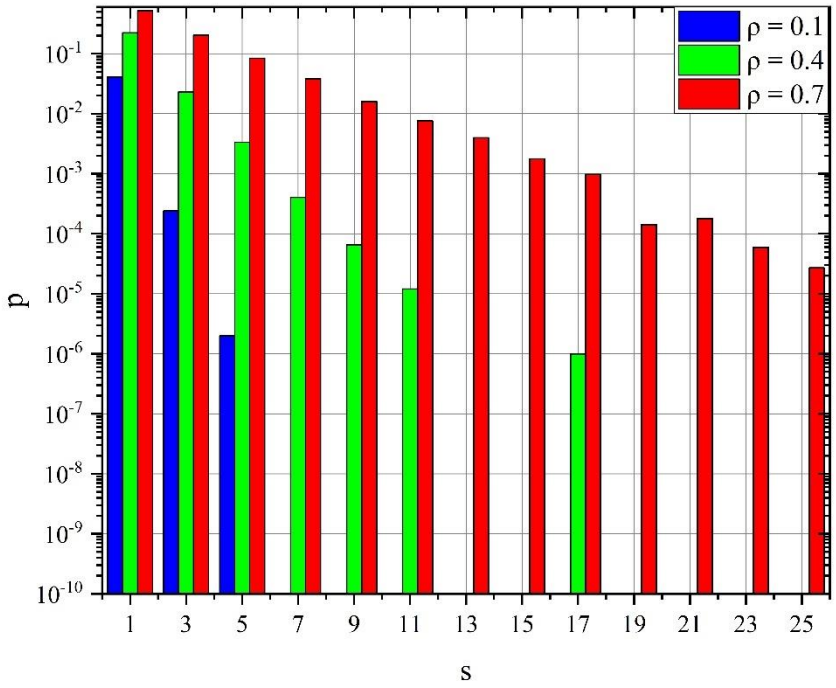
Εικόνα 4-5: Μεταβολή καθυστέρησης (L) ως συνάρτηση του αριθμού διαύλων πρόσβασης του συστήματος (s), σε B-RAN

Για συγκεκριμένη τιμή της παραμέτρου s, όχι μεγαλύτερη του κατωφλίου, φαίνεται ότι η αύξηση του ρ έχει ως συνέπεια την αύξηση της L, καθώς για συγκεκριμένο αριθμό καναλιών πρόσβασης, η αύξηση του αριθμού των αιτημάτων (τηλεπικοινωνιακής κίνησης) έχει ως αποτέλεσμα περισσότερα αιτήματα να αναμένουν για μεγαλύτερο χρονικό διάστημα. Στην Εικόνα 4-5 αυτό παρατηρείται ξεκάθαρα για $s \leq 5$.

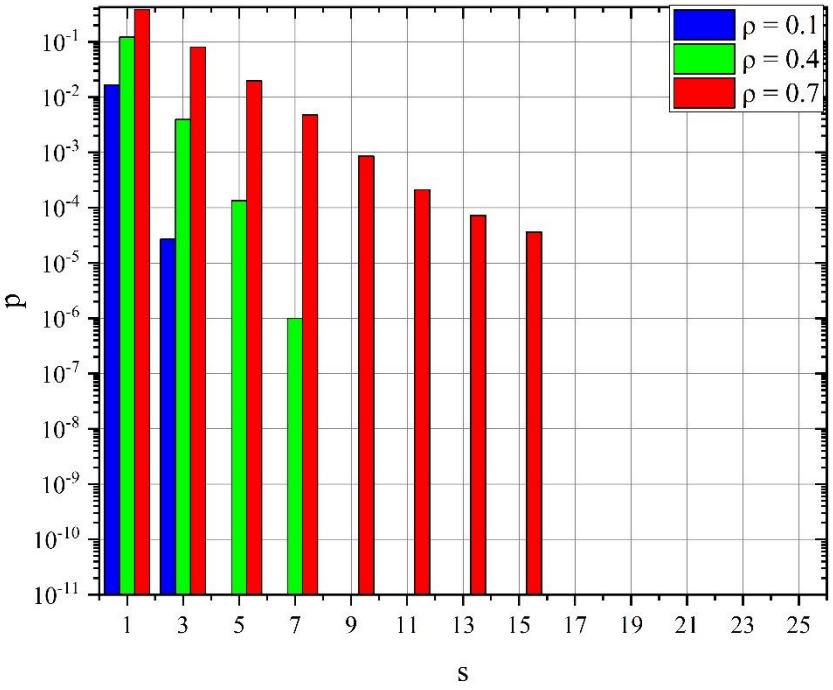
Η τρίτη προσομοίωση πραγματεύεται την επίδραση του αριθμού διαθέσιμων καναλιών πρόσβασης του συστήματος (s) στην πιθανότητα αναμονής (p) αιτήματος σε ουρά για περισσότερες από μία (Εικόνα 4-6), δύο (Εικόνα 4-7) ή τρεις (Εικόνα 4-8) χρονικές μονάδες, σε κατάσταση χαμηλής, μέτριας και υψηλής έντασης τηλεπικοινωνιακής κίνησης. Οι τιμές των υπόλοιπων παραμέτρων ταυτίζονται με αυτές της δεύτερης προσομοίωσης ($\lambda_b = 27$ και $N = 3$). Επίσης το s λαμβάνει τιμές στο διάστημα $[1,25]$, με βήμα αύξησης 2.



Εικόνα 4-6: Μεταβολή πιθανότητας αναμονής (p), μεγαλύτερης της μίας χρονικής μονάδας, ως συνάρτηση του αριθμού διαθέσιμων διαύλων πρόσβασης (s), σε B-RAN



Εικόνα 4-7: Μεταβολή πιθανότητας αναμονής (p), μεγαλύτερης των δύο χρονικών μονάδων, ως συνάρτηση του αριθμού διαθέσιμων διαύλων πρόσβασης (s), σε B-RAN



Εικόνα 4-8: Μεταβολή πιθανότητας αναμονής (p), μεγαλύτερης των τριών χρονικών μονάδων, ως συνάρτηση του αριθμού διαθέσιμων διαύλων πρόσβασης (s), σε B-RAN

Η Εικόνα 4-6 αφορά την πιθανότητα εισαγωγής επικυρωμένου αιτήματος στην ουρά αναμονής, δηλαδή την πιθανότητα το αίτημα να αναμείνει για μία ή περισσότερες χρονικές μονάδες, σε συνθήκες διαφορετικής έντασης τηλεπικοινωνιακής κίνησης. Γίνεται αντιληπτό ότι καθώς αυξάνεται το s, για δεδομένη τηλεπικοινωνιακή κίνηση και χωρίς μεταβολή των υπόλοιπων παραμέτρων, η p μειώνεται. Παραδείγματος χάρη, για $\rho = 0.4$ και $s = 1$, έχουμε $p = 0.402$, ενώ για το ίδιο ρ και $s = 5$, το p μειώνεται σε 0.062.

Για συγκεκριμένο s, αύξηση του ρ προκαλεί αύξηση του p. Είναι σαφές πως για μικρή τηλεπικοινωνιακή κίνηση η p γίνεται σύντομα σχεδόν αμελητέα (εδώ, για $s > 7$, στην περίπτωση όπου $\rho = 0.1$). Αντίθετα υπό συνθήκες αυξημένης τιμής του ρ, η p δεν θα μπορούσε να χαρακτηριστεί αμελητέα, ακόμα και όταν $s > 25$. Έτσι για $s = 3$, προκύπτει τιμή καθυστέρησης 0.004 όταν $\rho = 0.1$, 0.142 όταν $\rho = 0.4$ και 0.495 όταν $\rho = 0.7$.

Οι παραπάνω παρατηρήσεις μπορούν να ερμηνευθούν από το γεγονός ότι η ύπαρξη μεγαλύτερου πλήθους καναλιών πρόσβασης οδηγεί σε μείωση του αριθμού των αιτημάτων που απαιτείται να εισέλθουν στην ουρά αναμονής, καθώς θα βρουν ελεύθερο δίαυλο τη στιγμή της επικύρωσής τους, κατ' αναλογία και με την προηγούμενη περίπτωση.

Σε ότι αφορά την πιθανότητα αναμονής αιτήματος για δύο ή περισσότερες (Εικόνα 4-7), όπως και για τρεις ή περισσότερες χρονικές μονάδες (Εικόνα 4-8), οι παρατηρήσεις και οι ερμηνείες τους είναι παραπλήσιες με αυτές της προηγούμενης περίπτωσης. Όμως, όσο μεγαλώνει ο αριθμός των εξεταζόμενων χρονικών μονάδων καθυστέρησης, για τόσο μικρότερη τιμή του s θα παρατηρηθεί αμελητέα τιμή της p. Για παράδειγμα όταν ρ = 0.1, η τιμή του p γίνεται πολύ μικρή για $s > 7$, $s > 5$, $s > 3$, όταν εξετάζεται αναμονή πέρα της μίας, των δύο και των τριών χρονικών μονάδων, αντίστοιχα.

Τέλος, η πιθανότητα αναμονής δεν επηρεάζεται από τον απαιτούμενο αριθμό επιβεβαιώσεων για την επικύρωση των αιτημάτων, καθώς ο αριθμός αυτός, για μη ακραίες τιμές του, δε μεταβάλλει με κάποιον τρόπο το ρυθμό κατάληψης των καναλιών πρόσβασης του συστήματος, ούτε τη χρονική διάρκεια παραμονής των αιτημάτων στην ουρά αναμονής. Η αναμενόμενη αυτή συμπεριφορά του συστήματος επιβεβαιώθηκε και από τις προσομοιώσεις.

4.4 Συμπεράσματα

Στο παρόν κεφάλαιο παρουσιάστηκε το αναλυτικό μοντέλο περιγραφής της απλούστερης προτεινόμενης τοπολογίας του B-RAN. Η αναγωγή του σε μία χρονικά ομογενή διαδικασία Markov διευκολύνει σημαντικά τη μελέτη των ιδιοτήτων και των επιδόσεων του δικτύου.

Στη συνέχεια, με την εκτέλεση κατάλληλων προσομοιώσεων, αποδείχθηκε η ορθότητα του αναλυτικού μοντέλου και έγινε αποτίμηση των επιδόσεων του δικτύου, ως προς την καθυστέρηση και την πιθανότητα αναμονής. Παρατηρήθηκε λοιπόν ότι αυξάνοντας τον αριθμό των ελάχιστων απαιτούμενων επιβεβαιώσεων για την επικύρωση ενός αιτήματος, αυξάνεται και η καθυστέρηση πρόσβασης. Από την άλλη μεριά, μεγαλύτερος αριθμός επιβεβαιώσεων συνεπάγεται υψηλότερο επίπεδο ασφάλειας του συστήματος, οπότε μοιραία προκύπτει ένας συμβιβασμός (trade-off) μεταξύ της καθυστέρησης και της ασφάλειας του συστήματος. Επίσης φάνηκε πως ένας τρόπος μείωσης της καθυστέρησης είναι η παραχώρηση περισσότερων διαύλων πρόσβασης στο σύστημα, πράγμα που ισχύει μέχρι ενός σημείου, το οποίο εξαρτάται από την ένταση της τηλεπικοινωνιακής κίνησης, καθώς περαιτέρω αύξηση δεν μεταβάλλει σημαντικά τη καθυστέρηση. Όπως είναι λογικό, ανάλογη πτωτική τάση ακολουθεί και η πιθανότητα αναμονής, το ίδιο και οι χρονικές μονάδες για τις οποίες αυτή παρατηρείται, καθώς αυξάνονται οι διαθέσιμοι δίαυλοι πρόσβασης. Τέλος φάνηκε πως ένας ακόμα τρόπος μείωσης της καθυστέρησης είναι η αύξηση του ρυθμού γέννησης blocks.

Αξίζει να σημειωθεί ότι τα συμπεράσματα του κεφαλαίου αυτού έρχονται σε απόλυτη ταύτιση με αυτά του ερευνητικού άρθρου [30], πράγμα που ενισχύει την ορθότητά τους.

5 Έμμεση Πρόσβαση σε B-RAN

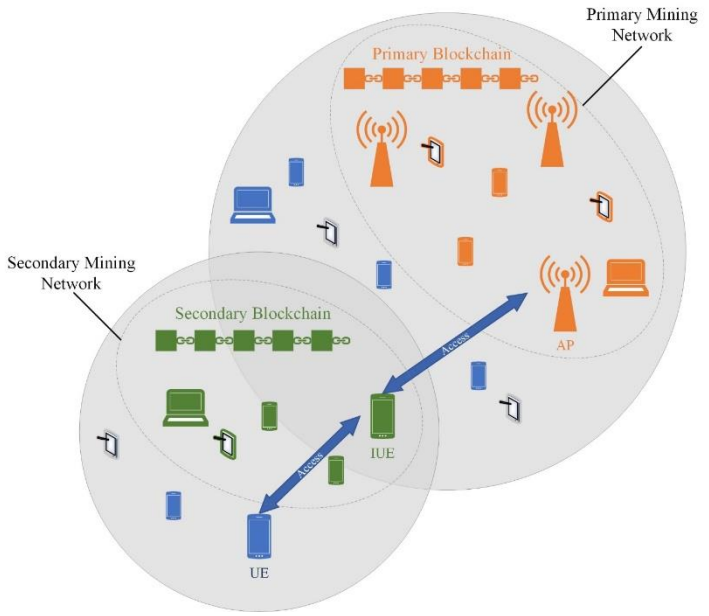
Βασική υπόσχεση των B5G τηλεπικοινωνιακών συστημάτων και θεμελιώδης προϋπόθεση του IoE είναι η πανταχού συνδεσιμότητα. Απαιτείται λοιπόν, ο κατά το δυνατόν περιορισμός των κενών κάλυψης (coverage holes), δηλαδή των περιοχών εκτός της εμβέλειας οιουδήποτε σημείου πρόσβασης του ασύρματου τηλεπικοινωνιακού συστήματος. Προς την κατεύθυνση αυτή, στο πλαίσιο της παρούσας διπλωματικής εργασίας, προτείνεται το DH-BRAN, ως μία τοπολογία παροχής έμμεσης πρόσβασης σε εκτός κάλυψης συσκευή (UE), με τη μεσολάβηση συσκευής άλλου συνδρομητή (IUE), ο οποίος διαθέτει το αντίστοιχο δικαίωμα.

Στο τρέχον κεφάλαιο, αρχικά αναλύεται η τοπολογία του DH-BRAN και το αντίστοιχο πρωτόκολλο έμμεσης πρόσβασης. Κατόπιν το DH-BRAN μοντελοποιείται ως μια διαδικασία Markov ομογενούς χρόνου, επεκτείνοντας το αντίστοιχο μοντέλο της άμεσης πρόσβασης που αναλύεται στο κεφάλαιο 4. Τέλος, με τη βοήθεια προσομοιώσεων, αποδεικνύεται η δυνατότητα πρακτικής υλοποίησης της προτεινόμενης τοπολογίας και αποτιμώνται οι επιδόσεις του αντίστοιχου πρωτοκόλλου. Στο σημείο αυτό, αξίζει να σημειωθεί ότι το παρόν κεφάλαιο αποτελεί την κύρια συνεισφορά της διπλωματικής εργασίας και μέρος του έχει δημοσιευθεί στο [44].

Ο κώδικας των προσομοιώσεων είναι διαθέσιμος στο GitHub [42].

5.1 Τοπολογία DH-BRAN και Πρωτόκολλο Έμμεσης Πρόσβασης

Το DH-BRAN, η τοπολογία του οποίου παρουσιάζεται στην Εικόνα 5-1, αυτό-δημιουργείται δυναμικά, κατά περίπτωση και κατανεμημένα, με τη συνεργασία δύο απλών B-RANs (κεφάλαιο 4), έστω του πρωτεύοντος και του δευτερεύοντος. Για λόγους σαφήνειας και χωρίς βλάβη της γενικότητας μπορεί να θεωρηθεί ότι στο πρωτεύον κάθε συσκευή συνδέεται απευθείας σε ένα συμβατικό AP του δικτύου (άμεση πρόσβαση), ενώ στο δευτερεύον κάθε σύνδεση πραγματοποιείται με τη μεσολάβηση κάποιας IUE (έμμεση πρόσβαση). Αρκετές εκτός κάλυψης UEs αναμένεται να βρίσκονται ενός της εμβέλειας κάποιας IUE που έχει δυνατότητα επικοινωνίας με συμβατικό AP, τη χρονική στιγμή που απαιτείται και προσφέρει αποδεκτό SLA. Με το μηχανισμό αυτό εγκαθίσταται επικοινωνία μεταξύ της UE και του AP, με τη μεσολάβηση της IUE.



Εικόνα 5-1 Τοπολογία DH-BRAN

Η προτεινόμενη τοπολογία DH-BRAN ενσωματώνει δύο ξεχωριστά blockchains, ένα στο πρωτεύον και ένα στο δευτερεύον B-RAN. Ακολουθώντας την προηγούμενη παραδοχή, στο πρωτεύον το mining και η επίτευξη ομοφωνίας είναι έργο των συμβατικών APs και προαιρετικά επιλεγμένων UEs. Στο δευτερεύον είναι έργο αποκλειστικά ορισμένων UEs που διαθέτουν την απαιτούμενη υπολογιστική ισχύ.

Το blockchain εγγυάται υψηλό επίπεδο ασφάλειας κατά τη μεταφορά δεδομένων μεταξύ μη έμπιστων οντοτήτων, επιτρέποντας την επεκτασιμότητα και τον κατά περίπτωση (ad-hoc) σχηματισμό του δικτύου. Πιο συγκεκριμένα, δίνεται η δυνατότητα σε κάθε συνδρομητή που το επιθυμεί και διαθέτει έξυπνη συσκευή με επαρκείς δυνατότητες να αποκτήσει το δικαίωμα παροχής έμμεσης πρόσβασης σε UE άλλου συνδρομητή, εξαλείφοντας τα πλέον προφανή προβλήματα που μπορούν να προκύψουν από πιθανή μη έντιμη συμπεριφορά του. Επιπλέον, είναι εγγυημένη η ασφαλής επικοινωνία μεταξύ οποιωνδήποτε συσκευών παίζουν το ρόλο των UE και IUE, καθώς οι όροι του προσυμφωνημένου SLA εφαρμόζονται αυτόματα και κατά περίπτωση, από τον κώδικα των έξυπνων συμβολαίων. Η IUE δεν έχει τη δυνατότητα προσπέλασης, τροποποίησης ή διαγραφής των δεδομένων που λαμβάνει και αναμεταδίδει κατά τη μεσολάβησή της μεταξύ UE και συμβατικού AP, πρόκληση που εμπόδισε την πρακτική υλοποίηση της έμμεσης πρόσβασης στο LTE.

Στο πλαίσιο της παρούσας εργασίας, προτείνεται ένα πρωτόκολλο έμμεσης πρόσβασης στο DH-BRAN, που εξάγεται επεκτείνοντας τη διαδικασία άμεσης πρόσβασης και αποτελείται από ένα προκαταρκτικό στάδιο και τα οκτώ παρακάτω βήματα (Εικόνα 5-2):

- **Προκαταρκτικό στάδιο:** Προκειμένου να αποκτήσει πρόσβαση στο δίκτυο μία εκτός κάλυψης UE, προχωρά σε αναζήτηση των διαθέσιμων IUE εντός της εμβέλειάς της. Για τη διευκόλυνση της αναζήτησης και της επιλογής κατάλληλης IUE, κάθε τέτοια συσκευή εκπέμπει περιοδικά ένα σήμα, δηλώνοντας την ύπαρξή της και τα βέλτιστα χαρακτηριστικά της σύνδεσης που έχει τη δυνατότητα να υποστηρίξει (ρυθμός δεδομένων, καθυστέρηση, κόστος, κ.α.).

- **Βήμα 1:** Η UE υποβάλλει ένα αίτημα έμμεσης πρόσβασης σε IUE της επιλογής της, αποδεχόμενη τις παραμέτρους της προσφερόμενης σύνδεσης. Το αίτημα αυτό καταγράφεται σε ένα έξυπνο συμβόλαιο, οπότε δημιουργείται ένα SLA μεταξύ των δυο μερών. Κατόπιν ελέγχεται, από τους miners του δευτερεύοντος δικτύου, η εγκυρότητα της συναλλαγής που περιλαμβάνει το έξυπνο συμβόλαιο.

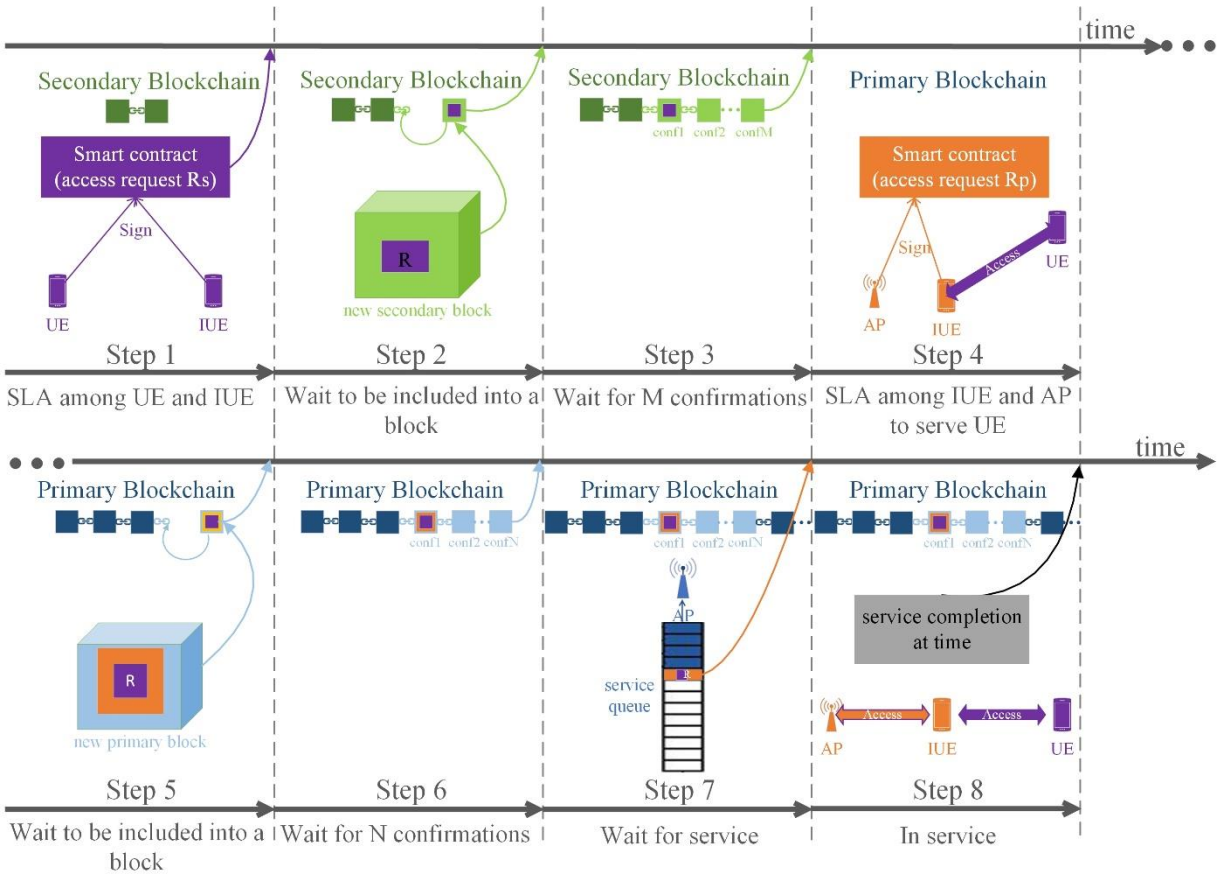
- **Βήμα 2:** Το προαναφερθέν συμβόλαιο περικλείεται στο επόμενο block που γεννάται στο δευτερεύον B-RAN, ενδεχομένως μαζί με άλλες ομοειδείς συναλλαγές (αιτήματα έμμεσης πρόσβασης). Στη συνέχεια το block προσαρτάται στο τέλος του δευτερεύοντος blockchain, οπότε το αίτημα λαμβάνει την πρώτη του επιβεβαίωση.

- **Βήμα 3:** Το αίτημα πρόσβασης «περιμένει» να λάβει τις ελάχιστες απαιτούμενες επιβεβαιώσεις (έστω M) ώστε να επικυρωθεί, δηλαδή η πληροφορία του να θεωρηθεί έγκυρη και ισχύουσα μεταξύ των miners του δευτερεύοντος B-RAN και να ενημερωθεί αναλόγως το DL του κάθε miner. Κάθε επιβεβαίωση λαμβάνεται με τη γέννηση ενός δευτερεύοντος block.

- **Βήμα 4:** Η IUE υποβάλλει ένα αίτημα στο συμβατικό AP όπου είναι συνδεδεμένη, το οποίο αφορά την παροχή πρόσβασης στη UE. Το αίτημα καταγράφεται σε ένα (διαφορετικό) έξυπνο συμβόλαιο, στο πρωτεύον B-RAN, το οποίο ορίζει το SLA μεταξύ IUE και AP. Κατόπιν ελέγχεται η εγκυρότητα του προκύπτοντος έξυπνου συμβολαίου (της συναλλαγής επίκλησης) από τους miners του πρωτεύοντος B-RAN.

- **Βήμα 5:** Το έξυπνο συμβόλαιο περικλείεται στο επόμενο block που γεννά κάποιος miner του πρωτεύοντος B-RAN. Ακολουθείται παρόμοια διαδικασία με αυτή που περιγράφεται στο βήμα 2 (η οποία λαμβάνει χώρα στο πρωτεύον δίκτυο αυτή τη φορά).

- **Βήμα 6:** Το block που δημιουργήθηκε κατά το προηγούμενο βήμα, λαμβάνει άλλες $N-1$ επιβεβαιώσεις (γεννήσεις πρωτευόντων blocks), οπότε ενημερώνεται το αντίγραφο της βάσης δεδομένων κάθε miner του πρωτεύοντος B-RAN με την αντίστοιχη πληροφορία.
- **Βήμα 7:** Εάν τη χρονική στιγμή έλευσης της N επιβεβαίωσης του αιτήματος, όλα τα κανάλια πρόσβασης του πρωτεύοντος δικτύου είναι κατειλημμένα, αυτό εισάγεται σε μία ουρά αναμονής, περιμένοντας την απελευθέρωση ενός καναλιού. Προφανώς, κάτι τέτοιο δεν συμβαίνει αναγκαστικά με κάθε αίτημα.
- **Βήμα 8:** Η UE αποκτά πρόσβαση στο τηλεπικοινωνιακό σύστημα, καθώς εγκαθίσταται σύνδεση μεταξύ αυτής και ενός συμβατικού AP, με τη μεσολάβηση της IUE. Οι όροι της πρόσβασης και της ποιότητας των παρεχόμενων υπηρεσιών καθορίζονται από τα έξυπνα συμβόλαια τόσο μεταξύ UE και IUE, όσο και μεταξύ IUE και AP.



Εικόνα 5-2: Βήματα πρωτοκόλλου έμμεσης πρόσβασης

5.2 Μοντελοποίηση Έμμεσης Πρόσβασης ως Διαδικασία Markov

Η παρούσα υπο-ενότητα αφιερώνεται στην τροποποίηση του μοντέλου Markov του B-RAN, που αναλύθηκε στο προηγούμενο κεφάλαιο, ώστε να περιγράψει την περίπτωση της έμμεσης πρόσβασης. Η λειτουργία του DH-BRAN βασίζεται ουσιαστικά στις ίδιες διαδικασίες (υποβολή αιτήματος, γέννηση block, περάτωση εξυπηρέτησης αιτήματος) που επιτελούνται κατά την άμεση πρόσβαση στο B-RAN, οπότε δεν διαφοροποιείται η στατιστική συμπεριφορά τους.

Έτσι οι διαδικασίες άφιξης αιτημάτων πρόσβασης, γέννησης blocks στο πρωτεύον και στο δευτερεύον B-RAN, καθώς και τερματισμού της εξυπηρέτησης αιτημάτων είναι στατιστικά ανεξάρτητες και ακολουθούν την κατανομή Poisson. Οι ρυθμοί τους ορίζονται ως λ_a, λ_{b1}, λ_{b2}, λ_c, αντίστοιχα. Επομένως, ο χρόνος μεταξύ της υποβολής δύο διαδοχικών αιτημάτων έμμεσης πρόσβασης στο δευτερεύον B-RAN ακολουθεί την εκθετική κατανομή, με μέση τιμή:

$$\mu_a = \frac{1}{\lambda_a}$$

Το ίδιο ισχύει για τους χρόνους μεταξύ δύο διαδοχικών γεννήσεων blocks στο πρωτεύον και το δευτερεύον B-RAN, με αντίστοιχες μέσες τιμές:

$$\mu_{b1} = \frac{1}{\lambda_{b1}}$$

$$\mu_{b2} = \frac{1}{\lambda_{b2}}$$

Τέλος ο χρόνος εξυπηρέτησης των αιτημάτων (από το πρωτεύον B-RAN) είναι επίσης εκθετικός, με μέση τιμή:

$$\mu_c = \frac{1}{\lambda_c}$$

Κατ' αναλογία με το κεφάλαιο 4, ο ρυθμός εμφάνισης γεγονότων θα ακολουθεί την κατανομή Poisson, με μέση τιμή:

$$\lambda = \lambda_a + \lambda_{b1} + \lambda_{b2} + \lambda_c$$

και επομένως ο μέσος χρόνος μεταξύ δύο οποιονδήποτε διαδοχικών γεγονότων (όχι απαραίτητα του ίδιου είδους) θα είναι εκθετικός, με μέση τιμή:

$$\mu = \frac{1}{\lambda}$$

Προκειμένου να κατασκευαστεί ένα αναλυτικό μοντέλο περιγραφής του πρωτόκολλου έμμεσης πρόσβασης, το πρωτεύων και το δευτερεύον B-RAN μπορούν να θεωρηθούν ως ενιαίο σύστημα. Με τη βοήθεια της Θεωρίας Ουρών Αναμονής, η κατάσταση του συστήματος κάθε χρονική στιγμή t περιγράφεται από ένα διάνυσμα της μορφής:

$$X(t) = E(j_0, j_1, \dots, j_{M-1}, i_0, i_1, \dots, i_{N-1}, k)$$

Όπου:

j_m: ο αριθμός των αιτημάτων πρόσβασης στο δευτερεύον B-RAN που έχουν λάβει m επιβεβαιώσεις έως τη χρονική στιγμή t

M: ο ελάχιστος αριθμός επιβεβαιώσεων που πρέπει να λάβει ένα αίτημα ώστε να θεωρηθεί επικυρωμένο, στο δευτερεύον B-RAN

i_n: ο αριθμός των αιτημάτων πρόσβασης στο πρωτεύον B-RAN που έχουν λάβει n επιβεβαιώσεις έως τη χρονική στιγμή t

N: ο ελάχιστος αριθμός επιβεβαιώσεων που πρέπει να λάβει ένα αίτημα ώστε να θεωρηθεί επικυρωμένο, στο πρωτεύον B-RAN

k: ο αριθμός των επικυρωμένων αιτημάτων πρόσβασης, που αναμένουν την απελευθέρωση καναλιού, ώστε να αποκτήσουν πρόσβαση

Καθώς το DH-BRAN μοντελοποιήθηκε κατ' αναλογία με την απλούστερη τοπολογία ενός B-RAN, όπου είναι εφικτή κατ' αποκλειστικότητα η άμεση πρόσβαση, το $X(t)$ θα είναι μία χρονικά ομογενής διαδικασία Markov και στην περίπτωση της έμμεσης πρόσβασης.

Η Εικόνα 5-3 παρουσιάζει το διάγραμμα μετάπτωσης καταστάσεων της τοπολογίας επίτευξης έμμεσης πρόσβασης (πρωτεύον και δευτερεύον B-RAN ως ενιαίο σύστημα). Έστω ότι τη χρονική στιγμή έναρξης της παρατήρησης του συστήματος (t) αυτό βρίσκεται στην αρχική κατάσταση:

$$X(t) = E_i(j_0, j_1, \dots, j_{M-1}, i_0, i_1, \dots, i_{N-1}, k)$$

Μετά τη διέλευση επαρκώς μικρού χρονικού διαστήματος (h), μπορεί να πραγματοποιηθεί μια και μόνο μία από τις παρακάτω μεταβάσεις:

- Με την **άφιξη ενός αιτήματος έμμεσης πρόσβασης**, τη χρονική στιγμή $(t + h)$ υπάρχει στο δευτερεύον B-RAN ένα επιπλέον αίτημα χωρίς καμία επιβεβαίωση, οπότε το σύστημα μεταβαίνει στην κατάσταση:

$$X(t + h) = E\big(j_0 + 1, j_1, \dots, j_{M-1}, i_{0,} i_1, \dots, i_{N-1}, k\big)$$

με πιθανότητα:

$$Pr(A) = \lambda_a h$$

Όπου: A το γεγονός άφιξης ενός αιτήματος πρόσβασης

- Με τη **γέννηση ενός block στο πρωτεύον B-RAN**, κάθε αίτημα που βρίσκεται σε αυτό λαμβάνει μία επιπλέον επιβεβαίωση, οπότε κανένα ανεπιβεβαίωτο αίτημα δεν βρίσκεται σε αυτό. Τα αιτήματα που λαμβάνουν την N-οστή επιβεβαίωση κατά τη χρονική στιγμή $(t + h)$ μπορούν να εξυπηρετηθούν άμεσα, εφόσον υπάρχει διαθέσιμο κανάλι. Έτσι, το σύστημα μεταβαίνει στην κατάσταση:

$$X(t + h) = E(j_0, j_1, \dots, j_{M-1}, 0, i_0, i_1, \dots, i_{N-1} + k)$$

με πιθανότητα:

$$Pr(B_1) = \lambda_{b1} h$$

Όπου B_1 το γεγονός γέννησης ενός block στο πρωτεύον B-RAN

- Με **τη γέννηση ενός block στο δευτερεύον B-RAN**, κάθε αίτημα σε αυτό λαμβάνει μία επιπλέον επιβεβαίωση, ανάλογα με την προηγούμενη περίπτωση. Εφόσον υπάρχουν αιτήματα που κατά τη χρονική στιγμή $(t + h)$ λαμβάνουν την επιβεβαίωση M, το δευτερεύον B-RAN υποβάλλει ένα αίτημα στο πρωτεύον, ζητώντας την παροχή πρόσβασης στις εκτός κάλυψης συσκευές. Στην περίπτωση αυτή το σύστημα μεταβαίνει στην κατάσταση:

$$X(t + h) = E(0, j_0, j_1, \dots, j_{M-2}, i_0 + j_{M-1}, i_1, \dots, i_{N-1}, k)$$

με πιθανότητα:

$$Pr(B_2) = \lambda_{b2} h$$

Όπου B_2 το γεγονός γέννησης ενός block στο πρωτεύον B-RAN

- Με την **ολοκλήρωση της εξυπηρέτησης ενός αιτήματος**, στο πρωτεύον B-RAN, το σύστημα μεταβαίνει στην κατάσταση:

$$X(t + h) = E\big(j_0, j_1, \dots, j_{M-1}, i_{0,} i_1, \dots, i_{N-1}, k - 1\big)$$

με πιθανότητα:

$$Pr(C) = \lambda_c h$$

Όπου: C το γεγονός της περάτωσης της εξυπηρέτησης ενός αιτήματος

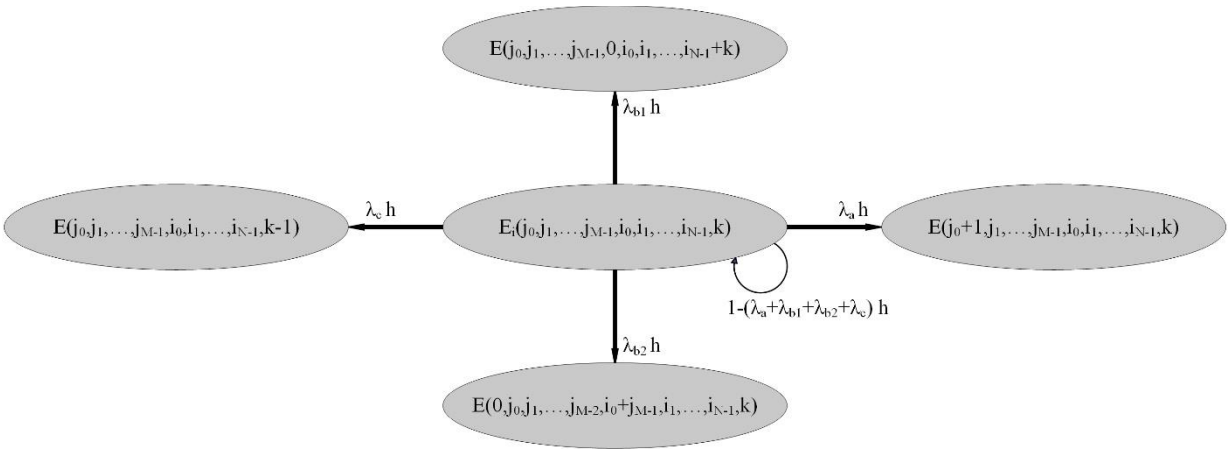
- Τέλος, το σύστημα παραμένει στην **ίδια κατάσταση**:

$$X(t+h) = E_i(t)$$

με πιθανότητα:

$$Pr(D) = 1 - (\lambda_a + \lambda_{b1} + \lambda_{b2} + \lambda_c)h$$

Όπου: το D αντιστοιχεί στην περίπτωση κατά την οποία η κατάσταση του συστήματος παραμένει αμετάβλητη



Εικόνα 5-3 Διάγραμμα μετάπτωσης καταστάσεων DH-BRAN

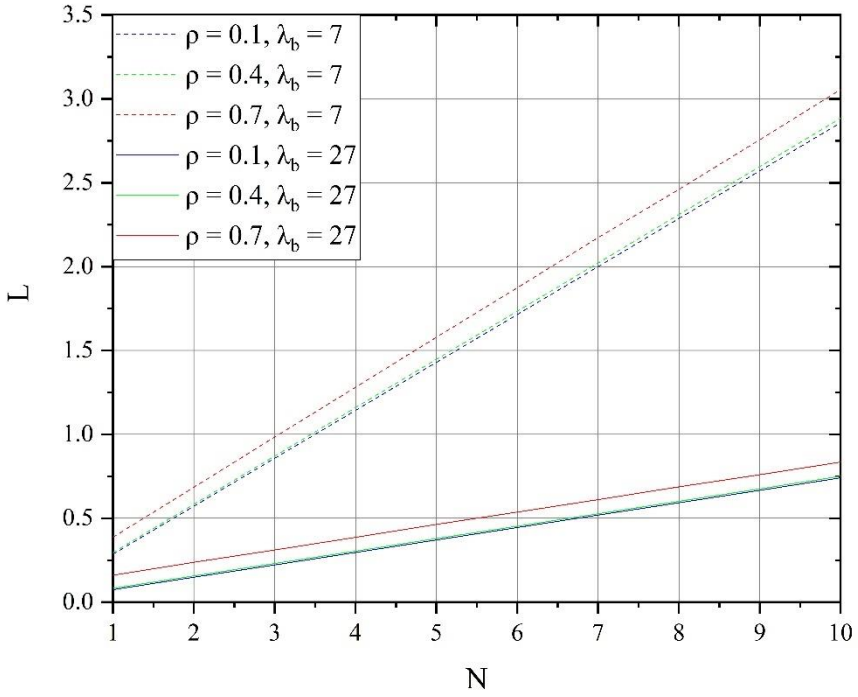
5.3 Αποτελέσματα Προσομοιώσεων

Η παρούσα υποενότητα αφιερώνεται στην ανάπτυξη προσομοιώσεων του DH-BRAN που αποσκοπούν στην απόδειξη της δυνατότητας πρακτικής υλοποίησής του και στην αποτίμηση των επιδόσεών του. Ως βασικοί KPIs χρησιμοποιούνται η μέση καθυστέρηση (L) και η πιθανότητα αναμονής (p), όπως ορίστηκαν στην προηγούμενη ενότητα.

Κατ' αντιστοιχία με το προηγούμενο κεφάλαιο κάθε προσομοίωση εκτελείται σε συνθήκες χαμηλής, μέτριας και υψηλής έντασης τηλεπικοινωνιακής κίνησης, με $\rho = 0.1$, $\rho = 0.4$ και $\rho = 0.7$, αντίστοιχα. Ως κριτήριο τερματισμού προσομοίωσης ορίζεται η ολοκλήρωση της εξυπηρέτησης ενός εκατομμυρίου αιτημάτων. Ο ρυθμός ολοκλήρωσης εξυπηρέτησης τίθεται ίσος με τη μονάδα ($\lambda_c = 1$), οπότε κάθε εξαγόμενο αποτέλεσμα εκφράζεται σε μονάδες λ_c.

Επισημαίνεται πως παρά το γεγονός ότι το πρωτεύον και το δευτερεύον B-RAN μοντελοποιούνται ως ενιαίο σύστημα, στην πραγματικότητα είναι δύο διακριτά δίκτυα. Οπότε οι παράμετροι λειτουργίας τους μπορούν να είναι οι ίδιες ή να διαφέρουν. Στην παρούσα εργασία οι τιμές των παραμέτρων αυτών ταυτίζονται για τα δύο δίκτυα, σε κάθε περίπτωση.

Η πρώτη προσομοίωση, τα αποτελέσματα της οποίας απεικονίζονται στο γράφημα της Εικόνα 5-4, αφορά τη σχέση του ελάχιστου αριθμού επιβεβαιώσεων αιτημάτων (N), καθώς αυτός μεταβάλλεται από 1 έως 10, με τη μέση καθυστέρηση (L). Ο αριθμός των διαθέσιμων διαύλων πρόσβασης του συστήματος τίθεται ίσος με 5, ενώ εξάγονται αποτελέσματα για ρυθμούς γέννησης blocks 7 και 27.

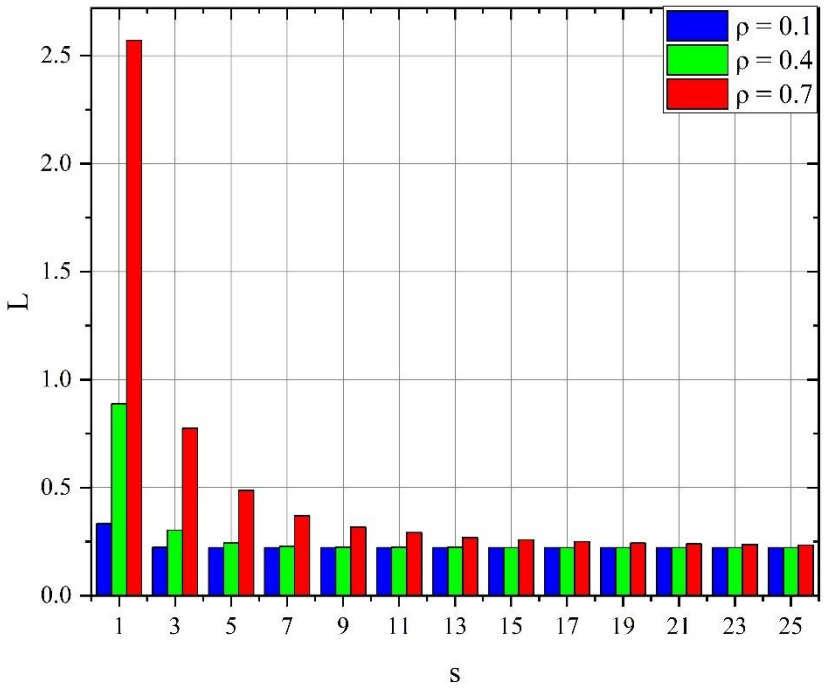


Εικόνα 5-4: Μεταβολή καθυστέρησης (L) ως συνάρτηση του ελάχιστου αριθμού επιβεβαιώσεων (N), σε DH-BRAN

Από την παραπάνω εικόνα, εξάγεται το συμπέρασμα ότι αύξηση της τιμής του N, διατηρώντας τις υπόλοιπες παραμέτρους σταθερές, έχει ως συνέπεια την αύξηση του L. Επίσης μεγαλύτερο ρ, στις ίδιες συνθήκες λειτουργίας του δικτύου, συνεπάγεται αύξηση της L. Ο μεγαλύτερος ρυθμός γέννησης blocks στο πρωτεύον και το δευτερεύον δίκτυο, ως ένα σημείο, έχει ως συνέπεια τη μείωση της καθυστέρησης. Η επεξήγηση των παραπάνω παρατηρήσεων είναι παρόμοια με αυτών της Εικόνα 4-4.

Όσο μεγαλύτερη είναι η τιμή του N, τόσο περισσότερες είναι οι μονάδες αύξησης της καθυστέρησης στην περίπτωση της έμμεσης πρόσβασης σε σύγκριση με την άμεση. Αυτό συμβαίνει επειδή ο χρόνος που απαιτείται ώστε να επιβεβαιωθεί περισσότερες φορές ένα αίτημα εισάγει καθυστέρηση τόσο στο πρωτεύον όσο και στο δευτερεύον B-RAN.

Η δεύτερη προσομοίωση, τα αποτελέσματα της οποίας παρουσιάζονται στην Εικόνα 5-5, αφορά την επίδραση του αριθμού των διαθέσιμων καναλιών πρόσβασης του συστήματος (s) στη μέση καθυστέρηση (L). Κατά τη συγκεκριμένη προσομοίωση, στο s ανατίθενται τιμές από 1 έως 25, με ρυθμό αύξησης 2, ο ρυθμός γεννήσεων blocks θεωρείται ίσος με 27, ενώ ο ελάχιστος αριθμός επιβεβαιώσεων ίσος με 3.

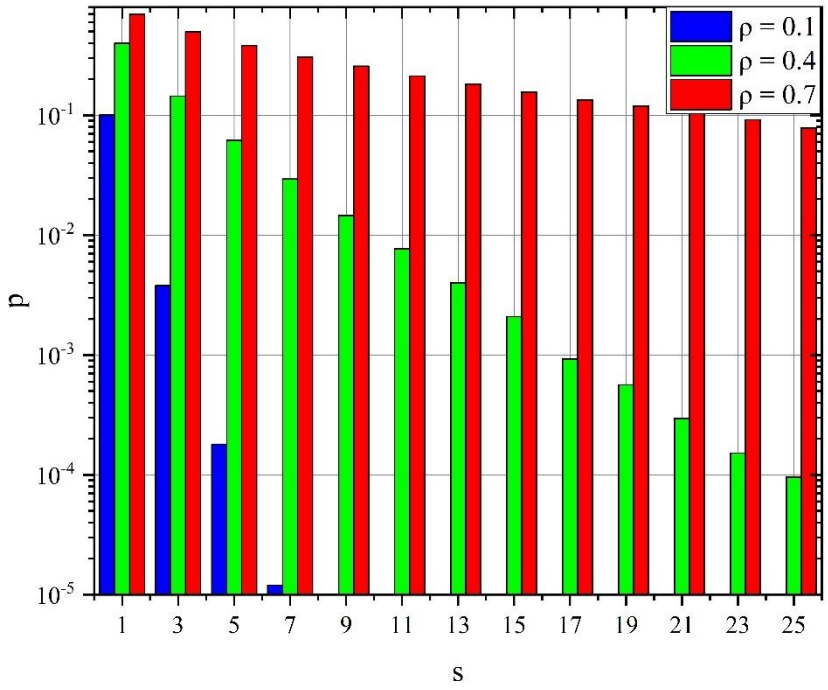


Εικόνα 5-5: Μεταβολή καθυστέρησης (L) ως συνάρτηση του αριθμού διαύλων πρόσβασης του συστήματος (s), σε DH-BRAN

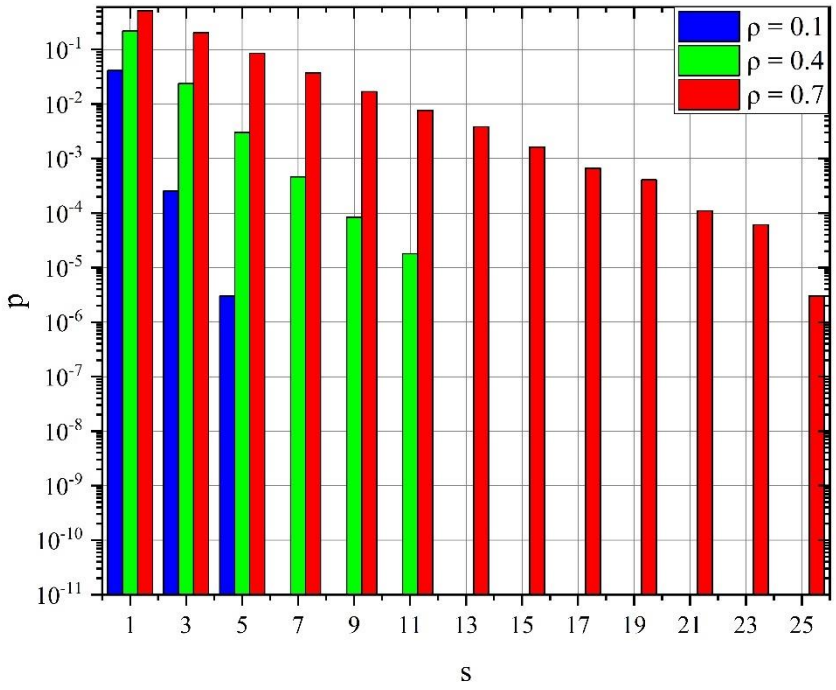
Στην εικόνα αυτή φαίνεται ότι η αύξηση του s, μέχρι ενός ορίου, διατηρώντας τις υπόλοιπες παραμέτρους σταθερές, οδηγεί σε μείωση της L. Από μία τιμή – κατώφλι και μετά, η αύξηση του s δεν επιδρά περεταίρω στην L. Επιπλέον, για συγκεκριμένη τιμή του s, υπό μεγαλύτερη τηλεπικοινωνιακή κίνηση παρατηρείται μεγαλύτερη μέση καθυστέρηση. Η τεκμηρίωση των παραπάνω παρατηρήσεων παρατίθεται στο κεφάλαιο 4, κατά την ανάλυση του γραφήματος της Εικόνα 4-5.

Γίνεται αντιληπτό ότι θεωρώντας τις ίδιες παραμέτρους για τις περιπτώσεις της άμεσης και της έμμεσης πρόσβασης, η επιπλέον καθυστέρηση που εισάγεται κατά την έμμεση διατηρείται περίπου σταθερή. Αυτό συμβαίνει επειδή ο αριθμός των διαθέσιμων καναλιών πρόσβασης δεν επηρεάζει τη λειτουργία του δευτερεύοντος δικτύου, οπότε η επιπλέον καθυστέρηση είναι ο χρόνος κατά τον οποίο το αίτημα παραμένει σε αυτό.

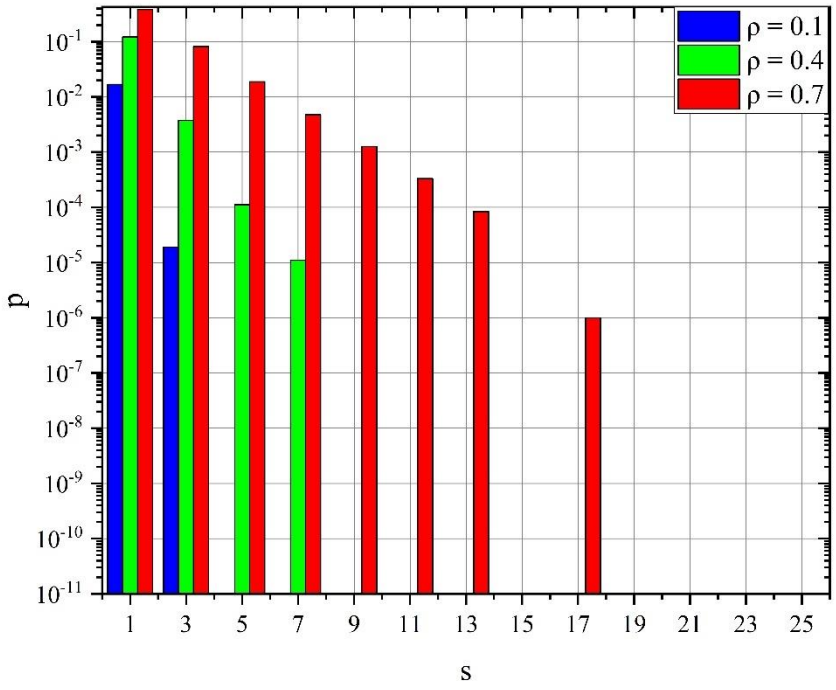
Τα αποτελέσματα της τρίτης προσομοίωσης παρουσιάζονται στα τρία επόμενα γραφήματα. Αυτή αφορά τη σχέση μεταξύ του αριθμού των διαθέσιμων καναλιών πρόσβασης του συστήματος (s) και της πιθανότητας αναμονής αιτήματος στην ουρά για περισσότερες από μία (Εικόνα 5-6), δύο (Εικόνα 5-7) ή τρεις (Εικόνα 5-8) χρονικές μονάδες. Οι τιμές των παραμέτρων επιλέγονται όμοιες με αυτές της δεύτερης προσομοίωσης.



Εικόνα 5-6: Μεταβολή πιθανότητας αναμονής (p), μεγαλύτερης της μίας χρονικής μονάδας, ως συνάρτηση του αριθμού διαθέσιμων διαύλων πρόσβασης (s), σε DH-BRAN



Εικόνα 5-7: Μεταβολή πιθανότητας αναμονής (p), μεγαλύτερης των δύο χρονικών μονάδων, ως συνάρτηση του αριθμού διαθέσιμων διαύλων πρόσβασης (s), σε DH-BRAN



Εικόνα 5-8: Μεταβολή πιθανότητας αναμονής (p), μεγαλύτερης των τριών χρονικών μονάδων, ως συνάρτηση του αριθμού διαθέσιμων διαύλων πρόσβασης (s), σε DH-BRAN

Τα αποτελέσματα που απεικονίζονται στα γραφήματα των εικόνων Εικόνα 5-6, Εικόνα 5-7, Εικόνα 5-8 είναι επίσης ανάλογα με τα αντίστοιχα που παρουσιάστηκαν στο κεφάλαιο 4. Φαίνεται λοιπόν ότι η αύξηση του s, με την ταυτόχρονη διατήρηση των υπόλοιπων εμπλεκόμενων μεγεθών, μειώνει την p. Επίσης, αύξηση της τιμής του ρ, αυξάνει και το p.

Σε ότι αφορά την εξέταση της πιθανότητας αναμονής για περισσότερες από δύο ή τρεις χρονικές μονάδες, παρατηρείται και πάλι ότι αυτή παρουσιάζεται αυξημένη υπό συνθήκες μεγαλύτερης τηλεπικοινωνιακής κίνησης. Αντίθετα για μικρές τιμές του ρ, μπορεί να θεωρηθεί αμελητέα.

Συγκρίνοντας τα σενάρια της έμμεσης και της άμεσης πρόσβασης μεταξύ τους, παρατηρείται ότι δεν υπάρχει σημαντική διαφορά, καθώς το επιπλέον βήμα της διαδικασίας (δευτερεύον δίκτυο) δεν επηρεάζει την πιθανότητα αναμονής.

5.4 Συμπεράσματα

Στο κεφάλαιο αυτό παρουσιάστηκε η τοπολογία DH-BRAN, που επιτυγχάνει την επέκταση της κάλυψης του δικτύου με την παροχή έμμεσης πρόσβασης σε συνδρομητή του οποίου η UE βρίσκεται σε σημείο εκτός κάλυψης. Μεσολαβεί η ήδη συνδεδεμένη συσκευή άλλου συνδρομητή, ο οποίος έχει το αντίστοιχο δικαίωμα. Κατά αντιστοιχία με την περίπτωση της άμεσης πρόσβασης στο B-RAN, αποδείχθηκε ότι το αναλυτικό μοντέλο περιγραφής του DH-BRAN ανάγεται σε μία χρονικά ομογενή διαδικασία Markov, πράγμα που διευκολύνει τη μελέτη των επιδόσεων και των ιδιαιτεροτήτων της συγκεκριμένης τοπολογίας.

Οι προσομοιώσεις του σεναρίου της άμεσης πρόσβασης επεκτάθηκαν και τροποποιήθηκαν, οπότε αποδείχθηκε η δυνατότητα πρακτικής υλοποίησης του προτεινόμενου πρωτοκόλλου έμμεσης πρόσβασης στο DH-BRAN. Σύμφωνα με τα εξαγόμενα αποτελέσματα, η συμπεριφορά των δύο εξεταζόμενων τοπολογιών, ως προς την καθυστέρηση και την πιθανότητα αναμονής, με τη μεταβολή βασικών παραμέτρων που χαρακτηρίζουν την κατάσταση και τη λειτουργία του δικτύου είναι παρόμοια. Ωστόσο στην περίπτωση του DH-BRAN, η καθυστέρηση εμφανίζεται αυξημένη και αυτό μπορεί να εξηγηθεί, καθώς για την ικανοποίηση ενός αιτήματος έμμεσης πρόσβασης γίνεται διπλή χρήση του blockchain, μία στο πρωτεύον και μία στο δευτερεύον B-RAN. Συνεπώς, το DH-BRAN είναι μία τοπολογία που υπόσχεται να επεκτείνει την κάλυψη των B5G, ενώ από αυτή φαίνεται να επωφελούνται ιδιαίτερα εφαρμογές με μικρές απαιτήσεις ως προς την καθυστέρηση.

6 Συμπεράσματα και Μελλοντικές Επεκτάσεις

Στο έκτο και τελευταίο, κεφάλαιο συνοψίζονται τα βασικότερα συμπεράσματα που προέκυψαν από την εκπόνηση της παρούσας διπλωματικής εργασίας και παρουσιάζονται μερικές πιθανές ερευνητικές κατευθύνσεις μελλοντικής επέκτασής της.

6.1 Σύνοψη Συμπερασμάτων

Η διαρκής και ραγδαία εξέλιξη των ασύρματων τηλεπικοινωνιακών συστημάτων συνεπάγεται την ταυτόχρονη αύξηση της πολυπλοκότητας του δικτύου και των προκλήσεων που πρέπει να αντιμετωπιστούν κατά τη σχεδίαση και τη λειτουργία του. Ειδικότερα για τα 5G and beyond ασύρματα δίκτυα, καίριες τέτοιες προκλήσεις αφορούν την ασφάλεια, την ακεραιότητα και την εμπιστευτικότητα των δεδομένων που διατηρούνται στο δίκτυο ή ανταλλάσσονται μεταξύ οντοτήτων αυτού. Γεγονός που ωθεί στην εξέταση της ενσωμάτωσης του blockchain σε ποικίλα σημεία του δικτύου.

Λαμβάνοντας ως κίνητρο το παραπάνω πρόβλημα, στην εργασία αυτή μελετήθηκε η ενσωμάτωση του blockchain στο τμήμα πρόσβασης των B5G συστημάτων. Προέκυψε λοιπόν η αρχιτεκτονική του B-RAN και το αναλυτικό μοντέλο περιγραφής της, που ανάγεται σε μία χρονικά ομογενή διαδικασία Markov. Ακόμα, διεξήχθησαν προσομοιώσεις για την αποτίμηση των επιδόσεων του συστήματος ως προς την καθυστέρηση και την πιθανότητα αναμονής, οπότε ήρθε στο φως η ύπαρξη ενός συμβιβασμού μεταξύ καθυστέρησης και ασφάλειας. Δηλαδή όσο μεγαλύτερος είναι ο αριθμός των επιβεβαιώσεων που λαμβάνει ένα αίτημα πρόσβασης ώστε να θεωρηθεί επικυρωμένο, τόσο βελτιώνεται το επίπεδο ασφάλειας του συστήματος. Όμως απαιτείται η πάροδος μεγαλύτερου χρονικού διαστήματος προκειμένου να ληφθούν οι επιπλέον επιβεβαιώσεις (γεννήσεις blocks). Για τον περιορισμό της καθυστέρησης προτείνεται η αύξηση του ρυθμού γέννησης blocks και η παροχή επαρκούς αριθμού διαύλων πρόσβασης στο σύστημα για τη συνήθη κατάσταση λειτουργίας του.

Πρωτοτυπία της εργασίας αποτελεί η υλοποίηση μίας τοπολογίας, του DH-BRAN, που αξιοποιείται ώστε να παρέχει έμμεση δικτυακή πρόσβαση σε συνδρομητή του οποίου η συσκευή βρίσκεται εκτός κάλυψης, με τη μεσολάβηση της ήδη συνδεδεμένης συσκευής άλλου συνδρομητή. Κατέστη λοιπόν φανερό ότι και το DH-BRAN δύναται να μοντελοποιηθεί ως μία διαδικασία Markov, ομογενούς χρόνου. Από τα αποτελέσματα των διεξαχθέντων προσομοιώσεων που επεκτάθηκαν για το σενάριο της έμμεσης πρόσβασης, διαφαίνεται ότι η

συμπεριφορά του DH-BRAN ως προς τις παραμέτρους της καθυστέρησης και της πιθανότητα αναμονής, είναι ανάλογη με αυτή του B-RAN. Παρατηρείται ωστόσο αυξημένη καθυστέρηση, καθώς το blockchain χρησιμοποιείται δύο φορές, μία κατά τη σύνδεση της συσκευής του αιτούντος συνδρομητή στη συσκευή που παίζει το ρόλο του μεσάζοντα και μία για τη μεταβίβαση του αιτήματος στο AP. Ακόμα, δεν παρατηρείται κάποια μεταβολή της πιθανότητας καθυστέρησης στην περίπτωση της έμμεσης πρόσβασης (DH-BRAN), συγκρινόμενη με την άμεση πρόσβαση σε συμβατικό AP του B-RAN, εάν ο αριθμός των διαθέσιμων διαύλων πρόσβασης του συστήματος διατηρηθεί αμετάβλητος.

6.2 Μελλοντικές Επεκτάσεις

Η διεξαχθείσα μελέτη, η καινοτομία του DH-BRAN και τα παραπάνω συμπεράσματα μπορούν να αποτελέσουν το υπόβαθρο μελλοντικών ερευνητικών επεκτάσεων.

Προς την κατεύθυνση αυτή, ιδιαίτερα χρήσιμη χαρακτηρίζεται η διερεύνηση των κατηγοριών εφαρμογών, για τις οποίες η επιπλέον καθυστέρηση ή άλλες επιβαρύνσεις που προκύπτουν από τη διαδικασία της έμμεσης πρόσβασης είναι ανεκτές. Επίσης θα μπορούσαν να αναζητηθούν τρόποι εξάλειψης ή μετριασμού των αδυναμιών αυτών.

Στο ίδιο πλαίσιο, θα μπορούσε να διεξαχθεί μελέτη της δυνατότητας και της χρησιμότητας επέκτασης της τοπολογίας έμμεσης πρόσβασης ώστε να εμπλέκει περισσότερες από δύο συσκευές, δημιουργώντας μια μεγαλύτερη αλυσίδα συσκευών που λειτουργούν ως μεσάζοντες. Εκ πρώτης όψεως, κάτι τέτοιο θα μπορούσε να φανεί χρήσιμο για εφαρμογές με σχετικά μικρές απαιτήσεις καθυστέρησης και ρυθμού δεδομένων, όπως αυτές που εκτελούνται σε συσκευές IoT.

Μία άλλη πιθανή μελλοντική επέκταση αποτελεί η μελέτη της αξιοποίησης του blockchain κατά την επικοινωνία μεταξύ τηλεπικοινωνιακών παρόχων που διαθέτουν διαφορετικού τύπου τηλεπικοινωνιακά συστήματα (επίγεια, εναέρια, υποθαλάσσια, ή δορυφορικά). Αυτό θα καταστήσει εφικτή την άμεση επικοινωνία τέτοιων συστημάτων και τη δρομολόγηση κίνησης μεταξύ αυτών, χωρίς τη μεσολάβηση κάποιας τρίτης οντότητας. Ο τρόπος επίτευξης αυτού του καθοριστικού για τα 6G στόχου, αναμένεται να παρουσιάζει σημαντικές ομοιότητες με την πρόσβαση μιας συσκευής στην απλή τοπολογία του B-RAN.

7 Βιβλιογραφία

[1] R. Yadav, ‘Challenges and Evolution of Next generation Wireless Communication’, *Hong Kong*, vol. 2, p. 5, 2017.

[2] S. Li, L. D. Xu, and S. Zhao, ‘5G Internet of Things: A survey’, *J. Ind. Inf. Integr.*, vol. 10, pp. 1–9, Jun. 2018, doi: 10.1016/j.jii.2018.01.005.

[3] D. C. Nguyen, ‘Blockchain for 5G and beyond networks: A state of the art survey’, *J. Netw. Comput. Appl.*, p. 38, 2020.

[4] X. Ling, J. Wang, T. Bouchoucha, B. C. Levy, and Z. Ding, ‘Blockchain Radio Access Network (B-RAN): Towards Decentralized Secure Radio Access Paradigm’, *IEEE Access*, vol. 7, pp. 9714–9723, 2019, doi: 10.1109/ACCESS.2018.2890557.

[5] S. Nakamoto, ‘Bitcoin: A Peer-to-Peer Electronic Cash System’, p. 9.

[6] J. Cope, ‘What’s a Peer-to-Peer (P2P) Network?’, *Computerworld*, Apr. 08, 2002. https://www.computerworld.com/article/2588287/networking-peer-to-peer-network.html (accessed Apr. 19, 2021).

[7] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, ‘An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends’, in *2017 IEEE International Congress on Big Data (BigData Congress)*, Honolulu, HI, USA, Jun. 2017, pp. 557–564. doi: 10.1109/BigDataCongress.2017.85.

[8] ‘A Beginner’s Introduction to Cryptoeconomics’, *Binance Academy*. https://academy.binance.com/en/articles/a-beginners-introduction-to-cryptoeconomics (accessed Apr. 21, 2021).

[9] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, ‘Blockchain’, *Bus. Inf. Syst. Eng.*, vol. 59, no. 3, pp. 183–187, Jun. 2017, doi: 10.1007/s12599-017-0467-3.

[10] I.-C. Lin and T.-C. Liao, ‘A Survey of Blockchain Security Issues and Challenges’, *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 653–659, Sep. 2017, doi: 10.6633/IJNS.201709.19(5).01.

[11] ‘What Is Cryptocurrency Mining?’, *Binance Academy*. https://academy.binance.com/en/articles/what-is-cryptocurrency-mining (accessed May 12, 2021).

[12] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, ‘A review on consensus algorithm of blockchain’, in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Banff, AB, Oct. 2017, pp. 2567–2572. doi: 10.1109/SMC.2017.8123011.

[13] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, 'Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends', *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 49, no. 11, pp. 2266–2277, Nov. 2019, doi: 10.1109/TSMC.2019.2895123.

[14] N. Szabo, 'Smart Contracts: Building Blocks for Digital Transformation'. 1996.

[15] E. Foundation, 'On Public and Private Blockchains'. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ (accessed Apr. 21, 2021).

[16] P. Tasatanattakool and C. Techapanupreeda, 'Blockchain: Challenges and applications', in *2018 International Conference on Information Networking (ICOIN)*, Chiang Mai, Thailand, Jan. 2018, pp. 473–475. doi: 10.1109/ICOIN.2018.8343163.

[17] M. Hölbl, M. Kompara, A. Kamišalić, and L. Nemec Zlatolas, 'A Systematic Review of the Use of Blockchain in Healthcare', *Symmetry*, vol. 10, no. 10, p. 470, Oct. 2018, doi: 10.3390/sym10100470.

[18] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, 'Blockchain technology and its relationships to sustainable supply chain management', *Int. J. Prod. Res.*, vol. 57, no. 7, pp. 2117–2135, Apr. 2019, doi: 10.1080/00207543.2018.1533261.

[19] N. Wang *et al.*, 'When Energy Trading Meets Blockchain in Electrical Power System: The State of the Art', *Appl. Sci.*, vol. 9, no. 8, p. 1561, Apr. 2019, doi: 10.3390/app9081561.

[20] A. Gupta and R. K. Jha, 'A Survey of 5G Network: Architecture and Emerging Technologies', *IEEE Access*, vol. 3, pp. 1206–1232, 2015, doi: 10.1109/ACCESS.2015.2461602.

[21] K. David and H. Berndt, '6G Vision and Requirements: Is There Any Need for Beyond 5G?', *IEEE Veh. Technol. Mag.*, vol. 13, no. 3, pp. 72–80, Sep. 2018, doi: 10.1109/MVT.2018.2848498.

[22] 'LTE'. https://www.3gpp.org/technologies/keywords-acronyms/98-lte (accessed Jul. 04, 2021).

[23] 'IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond', p. 21.

[24] 'Software-Defined Networking: The New Norm for Networks'. 2012. [Online]. Available: http://opennetworking.wpengine.com/wp-content/uploads/2011/09/wp-sdn-newnorm.pdf

[25] 'Network Functions Virtualisation'. 2012. [Online]. Available: https://portal.etsi.org/NFV/NFV_White_Paper.pdf

[26] T. Huang, W. Yang, J. Wu, J. Ma, X. Zhang, and D. Zhang, 'A Survey on Green 6G Network: Architecture and Technologies', *IEEE Access*, vol. 7, pp. 175758–175768, 2019, doi: 10.1109/ACCESS.2019.2957648.

[27] T. Hewa, G. Gur, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, 'The Role of Blockchain in 6G: Challenges, Opportunities and Research Directions', in *2020 2nd 6G Wireless*

Summit (6G SUMMIT), Levi, Finland, Mar. 2020, pp. 1–5. doi: 10.1109/6GSUMMIT49458.2020.9083784.

[28] X. Ling, J. Wang, Y. Le, Z. Ding, and X. Gao, 'Blockchain Radio Access Network Beyond 5G', *IEEE Wirel. Commun.*, vol. 27, no. 6, pp. 160–168, Dec. 2020, doi: 10.1109/MWC.001.2000172.

[29] Y. Le, X. Ling, J. Wang, and Z. Ding, 'Prototype Design and Test of Blockchain Radio Access Network', in *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*, Shanghai, China, May 2019, pp. 1–6. doi: 10.1109/ICCW.2019.8757042.

[30] X. Ling, Y. Le, J. Wang, Z. Ding, and X. Gao, 'Practical Modeling and Analysis of Blockchain Radio Access Network', *ArXiv191112537 Cs*, Nov. 2019, Accessed: May 28, 2021. [Online]. Available: http://arxiv.org/abs/1911.12537

[31] E. Di Pascale, J. McMenamy, I. Macaluso, and L. Doyle, 'Smart Contract SLAs for Dense Small-Cell-as-a-Service', *ArXiv170304502 Cs*, Mar. 2017, Accessed: Jul. 03, 2021. [Online]. Available: http://arxiv.org/abs/1703.04502

[32] B. Mafakheri, T. Subramanya, L. Goratti, and R. Riggio, 'Blockchain-based Infrastructure Sharing in 5G Small Cell Networks', *Poster Sess.*, p. 5, 2018.

[33] M. B. H. Weiss, K. Werbach, D. C. Sicker, and C. E. C. Bastidas, 'On the Application of Blockchains to Spectrum Management', *IEEE Trans. Cogn. Commun. Netw.*, vol. 5, no. 2, pp. 193–205, Jun. 2019, doi: 10.1109/TCCN.2019.2914052.

[34] P. Gorla, V. Chamola, V. Hassija, and N. Ansari, 'Blockchain Based Framework for Modeling and Evaluating 5G Spectrum Sharing', *IEEE Netw.*, vol. 35, no. 2, pp. 229–235, Mar. 2021, doi: 10.1109/MNET.011.2000469.

[35] X. Xu, Y. Chen, X. Zhang, Q. Liu, X. Liu, and L. Qi, 'A blockchain-based computation offloading method for edge computing in 5G networks', *Softw. Pract. Exp.*, p. spe.2749, Sep. 2019, doi: 10.1002/spe.2749.

[36] N. Weerasinghe, T. Hewa, M. Dissanayake, M. Ylianttila, and M. Liyanage, 'Blockchain-based Roaming and Offload Service Platform for Local 5G Operators', in *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, Jan. 2021, pp. 1–6. doi: 10.1109/CCNC49032.2021.9369516.

[37] X. Ling, Y. Le, J. Wang, and Z. Ding, 'Hash Access: Trustworthy Grant-Free IoT Access Enabled by Blockchain Radio Access Networks', *IEEE Netw.*, vol. 34, no. 1, pp. 54–61, Jan. 2020, doi: 10.1109/MNET.001.1900159.

[38] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, 'Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges', *IEEE Commun. Surv. Tutor.*, vol. 22, no. 4, pp. 2521–2549, 2020, doi: 10.1109/COMST.2020.3020092.

[39] P.-H. Kuo, A. Mourad, and J. Ahn, ‘Potential Applicability of Distributed Ledger to Wireless Networking Technologies’, *IEEE Wirel. Commun.*, vol. 25, no. 4, pp. 4–6, Aug. 2018, doi: 10.1109/MWC.2018.8454517.

[40] A. Azari, P. Popovski, G. Miao, and C. Stefanovic, ‘Grant-Free Radio Access for Short-Packet Communications over 5G Networks’, in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, Singapore, Dec. 2017, pp. 1–7. doi: 10.1109/GLOCOM.2017.8255054.

[41] Y. Liu, K. Wang, Y. Lin, and W. Xu, ‘$\mathsf{LightChain}$: A Lightweight Blockchain System for Industrial Internet of Things’, *IEEE Trans. Ind. Inform.*, vol. 15, no. 6, pp. 3571–3581, Jun. 2019, doi: 10.1109/TII.2019.2904049.

[42] Theofilos1997, *Theofilos1997/BRAN_DHBRAN_Simulations*. 2021. Accessed: Jul. 04, 2021. [Online]. Available: https://github.com/Theofilos1997/BRAN_DHBRAN_Simulations

[43] R. B. Cooper, ‘Queueing theory’, in *Proceedings of the ACM ’81 conference*, New York, NY, USA, Jan. 1981, pp. 119–122. doi: 10.1145/800175.809851.

[44] T. Sachinidis, A.-A. A. Boulogeorgos, and P. Sarigiannidis, ‘Dual-hop Blockchain Radio Access Networks for Advanced Coverage Expansion’, p. 5.