



ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
«ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΚΑΙ ΜΗΧΑΝΙΣΜΟΙ
ΣΥΝΑΙΝΕΣΗΣ ΤΟΥ SHIMMER NETWORK: ΑΝΑΛΥΣΗ
ΤΗΣ DLT ΥΠΟΔΟΜΗΣ ΔΙΕΡΕΥΝΗΣΗ ΕΡΕΥΝΗΤΙΚΩΝ ΠΡΟΚΛΗΣΕΩΝ ΚΑΙ
ΠΕΡΙΠΤΩΣΕΙΣ ΧΡΗΣΗΣ »

Της φοιτήτριας Μαυροματίδου
Ελένης
Αρ. Μητρώου: 2020092

Επιβλέπων Ονοματεπώνυμο
Αγγελόπουλος Μάριος

Ημερομηνία 01/09/2026

Τίτλος Δ.Ε. Αρχιτεκτονική και μηχανισμοί συναίνεσης του Shimmer network

Κωδικός Δ.Ε. 26128

Ονοματεπώνυμο φοιτητή Μαυροματίδου Ελένη

Ονοματεπώνυμο εισηγητή Αγγελόπουλος Μάριος

Ημερομηνία ανάληψης Δ.Ε. 25/02/2026

Ημερομηνία περάτωσης Δ.Ε.06/09/2026

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

Η παρούσα εργασία αποτελεί πνευματική ιδιοκτησία της φοιτήτριας Μαυροματίδου Ελένης που την εκπόνησε/αν. Στο πλαίσιο της πολιτικής ανοικτής πρόσβασης, ο συγγραφέας/δημιουργός εκχωρεί στο Διεθνές Πανεπιστήμιο της Ελλάδος άδεια χρήσης του δικαιώματος αναπαραγωγής, δανεισμού, παρουσίασης στο κοινό και ψηφιακής διάχυσης της εργασίας διεθνώς, σε ηλεκτρονική μορφή και σε οποιοδήποτε μέσο, για διδακτικούς και ερευνητικούς σκοπούς, άνευ ανταλλάγματος. Η ανοικτή πρόσβαση στο πλήρες κείμενο της εργασίας, δεν σημαίνει καθ' οιονδήποτε τρόπο παραχώρηση δικαιωμάτων διανοητικής ιδιοκτησίας του συγγραφέα/δημιουργού, ούτε επιτρέπει την αναπαραγωγή, αναδημοσίευση, αντιγραφή, πώληση, εμπορική χρήση, διανομή, έκδοση, μεταφόρτωση (downloading), ανάρτηση (uploading), μετάφραση, τροποποίηση με οποιονδήποτε τρόπο, τμηματικά ή περιληπτικά της εργασίας, χωρίς τη ρητή προηγούμενη έγγραφη συναίνεση του συγγραφέα/δημιουργού.

Η έγκριση της διπλωματικής εργασίας από το Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του Διεθνούς Πανεπιστημίου της Ελλάδος, δεν υποδηλώνει απαραίτητως και αποδοχή των απόψεων του συγγραφέα, εκ μέρους του Τμήματος.

«Αφιέρωση»

Πρόλογος

Η ραγδαία εξέλιξη του Διαδικτύου των Πραγμάτων (IoT) και η ανάγκη για ασφαλή, κλιμακώσιμη και αποκεντρωμένη διαχείριση δεδομένων αποτέλεσαν το βασικό κίνητρο για την επιλογή του θέματος της παρούσας διπλωματικής εργασίας. Ενώ οι παραδοσιακές τεχνολογίες Blockchain προσφέρουν σημαντικές λύσεις, οι περιορισμοί τους ως προς την επεκτασιμότητα και τα τέλη συναλλαγών με οδήγησαν να μελετήσω τις Τεχνολογίες Κατανεμημένου Καθολικού (DLT) που βασίζονται σε Κατευθυνόμενα Ακυκλικά Γραφήματα (DAG).

Η εστίαση στο οικοσύστημα του IOTA και ειδικότερα στο Shimmer Network με συνάρπασε, καθώς αποτελεί την αιχμή της τεχνολογίας, εισάγοντας καινοτόμους μηχανισμούς συναίνεσης και μια αρχιτεκτονική ιδανική για συσκευές με περιορισμένους πόρους.

Μέσα από την εκπόνηση αυτής της εργασίας, το όφελος ήταν πολλαπλό. Αρχικά, απέκτησα βαθιά κατανόηση της αρχιτεκτονικής των DAG-based DLT συστημάτων και των προκλήσεων ασφάλειας και επεκτασιμότητας που αυτά καλούνται να αντιμετωπίσουν. Παράλληλα, εξοικειώθηκα με τη μεθοδολογία της συστηματικής βιβλιογραφικής ανασκόπησης, αναπτύσσοντας ερευνητικές δεξιότητες. Τέλος, η πρόταση ενός πλαισίου επιλογής αρχιτεκτονικής για εφαρμογές IoT μου επέτρεψε να συνδυάσω τη θεωρητική γνώση με την πρακτική εφαρμογή, προετοιμάζοντάς με ουσιαστικά για τις μελλοντικές τεχνολογικές προκλήσεις στον τομέα των μηχανικών πληροφορικής.

Περίληψη

Η παρούσα εργασία στοχεύει στον να παράσχει μια ολοκληρωμένη εικόνα για τις τρέχουσες προσεγγίσεις που αφορούν την αρχιτεκτονική των DAG-based DLT συστημάτων και τους μηχανισμούς Συναίνεσης του Shimmer Network μέσω μιας επισταμένης βιβλιογραφικής επισκόπησης. Το IOTA είναι μια Τεχνολογία Κατανεμημένου Καθολικού (DLT) σχεδιασμένη για το Διαδίκτυο των Πραγμάτων (IoT), η οποία διαθέτει ανέπαφες συναλλαγές και μπλοκ δεδομένων για την κοινή χρήση πληροφοριών μεταξύ συσκευών IoT. Το κύριο συστατικό του IOTA είναι το Tangle το οποίο βασίζεται στην έννοια ενός Κατευθυνόμενου Ακυκλικού Γραφήματος (Directed Acyclic Graph DAG), που του επιτρέπει να κλιμακώνεται διατηρώντας παράλληλα την ασφάλεια, προσαρμοσμένη στις ανάγκες της ανάπτυξης του IoT. Η Τεχνολογία Κατανεμημένου Καθολικού (DLT) είναι μια αναδύομενη εξέλιξη που μοιράζεται δεδομένα μεταξύ διαφορετικών συμμετεχόντων που αναπτύσσονται σε διάφορες τοποθεσίες σε όλο τον κόσμο. Το Shimmer Network είναι ένα πειραματικό blockchain δίκτυο (DLT) που ανήκει στο οικοσύστημα του IOTA, και αποσκοπεί στην απρόσκοπτη σύνδεση έξυπνων αλυσίδων συμβολαίων. Αυτός όμως ο ταχέως αναπτυσσόμενος τομέας του Διαδικτύου των Πραγμάτων (IoT), και η ευρεία υιοθέτηση αυτών των τεχνολογιών αντιμετωπίζει σημαντικές προκλήσεις, που αφορούν τη διαχείριση ταυτοτήτων, το απόρρητο των δεδομένων και την ασφάλεια. Επειδή το blockchain είναι ένα δυναμικό, αυτορρυθμιζόμενο σύστημα, απαιτείται η ενσωμάτωση ενός ασφαλούς μηχανισμού για να διασφαλίσει την αυθεντικότητα των συναλλαγών, με το δεδομένο ότι οι συμμετέχοντες έχουν καταλήξει σε συμφωνία για συναίνεση. Έχουν προταθεί διάφοροι τύποι μηχανισμών συναίνεσης οι οποίοι διαφέρουν μεταξύ τους ως προς τις βασικές αρχές και εφαρμογές τους. Έχουν προταθεί τρεις κατηγορίες πρωτοκόλλων συναίνεσης όπως αυτά που βασίζονται στην απόδειξη εργασίας (PoW), αυτά που αντικαθιστούν την απόδειξη εργασίας με πιο ενεργειακά αποδοτικές εναλλακτικές λύσεις (PoX) και τέλος υβριδικά πρωτόκολλα. Υπάρχουν τα παραδοσιακά πρωτόκολλα blockchain, όπως η συναίνεση Nakamoto που εφαρμόζεται στο δίκτυο Bitcoin, ενώ ακολούθως προτάθηκαν και άλλα. Τα συστήματα αυτά όμως αντιμετωπίζουν προκλήσεις όπως η ασφάλεια, η επεκτασιμότητα, η ιδιωτικότητα, η προσβασιμότητα κ.ά.

«Τίτλος Διπλωματικής Εργασίας»

(Shimmer Network Architecture and Consensus Mechanisms: DLT
Infrastructure Analysis, Research Challenges Exploration and Use
Cases)

«Eleni Mavromatidou»

Abstract

This thesis aims to provide a comprehensive overview of current approaches concerning the architecture of DAG-based DLT systems and the consensus mechanisms of the Shimmer Network through an in-depth literature review. IOTA is a Distributed Ledger Technology (DLT) designed for the Internet of Things (IoT), featuring feeless transactions and data blocks for sharing information among IoT devices. The main component of IOTA is the Tangle, which is based on the concept of a Directed Acyclic Graph (DAG), enabling it to scale while maintaining security, tailored to the needs of IoT development. Distributed Ledger Technology (DLT) is an emerging development that enables data to be shared among different participants deployed across various locations worldwide. The Shimmer Network is an experimental blockchain network, or DLT, within the IOTA ecosystem, aiming to enable the seamless connection of smart contract chains. However, this rapidly evolving field of the Internet of Things (IoT), and the widespread adoption of these technologies, faces significant challenges related to identity management, data privacy, and security. Since blockchain is a dynamic, self-regulating system, the integration of a secure mechanism is required to ensure the authenticity of transactions, on the condition that participants have reached agreement through consensus. Consensus is used to maintain agreement among nodes in the network. Various types of consensus mechanisms have been proposed, differing in their fundamental principles and applications. Three categories of consensus protocols have been proposed: those based on Proof of Work (PoW), those that replace Proof of Work with more energy-efficient alternatives (PoX), and hybrid protocols, which are usually variations of classical consensus protocols. Traditional blockchain protocols also exist, such as Nakamoto consensus, which is implemented in the Bitcoin network, while others were subsequently proposed. However, these systems face challenges such as security, scalability, privacy, accessibility, and others.

Ευχαριστίες

Η παρούσα διπλωματική εργασία ολοκληρώθηκε με την επιστημονική υποστήριξη του επιβλέποντα καθηγητή μου, κ. Αγγελόπουλο Μάριο, τον οποίο και ευχαριστώ για τις κατευθύνσεις και τις συμβουλές του. Επιπλέον, θα ήθελα να εκφράσω την ειλικρινή μου ευγνωμοσύνη στην οικογένειά μου για την αμέριστη συμπαράσταση και την υπομονή της όλα αυτά τα χρόνια.

Περιεχόμενα

Πρόλογος.....	3
Περίληψη.....	4
Abstract.....	5
Ευχαριστίες.....	6
Περιεχόμενα.....	7
Κατάλογος Σχημάτων.....	9
Κατάλογος Πινάκων.....	9
Συντομογραφίες.....	10
Κεφάλαιο 1ο: Εισαγωγή.....	12
Κεφάλαιο 2ο: Βασικό Υπόβαθρο του IOTA και του Shimmer network.....	14
Κεφάλαιο 3ο: Μεθοδολογία συστηματικής βιβλιογραφικής ανασκόπησης.....	17
Κεφάλαιο 4ο: Αρχιτεκτονική των DAG-based DLT συστημάτων.....	20
4.1 Παραδοσιακή αρχιτεκτονική Blockchain.....	20
4.2 Αρχιτεκτονικές DAG-based DLT.....	22
4.3 IOTA Tangle.....	24
4.4 Αρχιτεκτονική κόμβων και διάδοση συναλλαγών.....	29
4.5 Stardust protocol.....	30
4.6 Shimmer Network architecture.....	30
4.7 ShimmerEVM και L1/L2 integration.....	31
4.8 Συγκριτική αποτίμηση Blockchain–DAG–Shimmer.....	34
Κεφάλαιο 5ο: Πρωτόκολλα Συναίνεσης.....	37
5.1 Πρωτόκολλα Συναίνεσης.....	37
5.2 Συναίνεση σε κλασικά blockchain.....	37
5.3 Γιατί τα DAG χρειάζονται διαφορετική προσέγγιση όσον αφορά τα πρωτόκολλα συναίνεσης.....	39
5.4 Συμβουλές για την επιλογή του πρωτοκόλλου συναίνεσης.....	40
5.5 FPC / συναίνεση πιθανοτήτων.....	42
5.6 Byzantine Fault Tolerance και DAG.....	44
5.7 Επίλυση συγκρούσεων.....	44
5.8 Σύγκριση μηχανισμών.....	44
Κεφάλαιο 6ο: Προκλήσεις (ασφάλεια, επεκτασιμότητα, ιδιωτικότητα)Αρχιτεκτονική των DAG-based DLT συστημάτων.....	48

6.1	Ασφάλεια	48
6.2	Επιθέσεις	49
6.3	Επεκτασιμότητα	50
6.4	Ιδιωτικότητα	52
6.5	Διπλές δαπάνες- αντικρουόμενες συναλλαγές	53
6.6	Διαλειτουργικότητα	53
Κεφάλαιο 7ο: Εφαρμογές - Περιπτώσεις Χρήσεις		55
7.1	IoT συλλογή-ανταλλαγή δεδομένων	56
7.2	Ασφάλεια Δεδομένων μέσω του Tangle	56
7.3	Υγειονομική Περίθαλψη και Διαδίκτυο των Πραγμάτων (IoT)	57
7.4	Ψηφιακή ταυτότητα / έλεγχος πρόσβασης	58
7.5	Κινητικότητα και Διαλειτουργικότητα DLT	59
7.6	Αγορές δεδομένων	60
7.7	Ηλεκτρονική ψηφοφορία με ShimmerEVM	60
7.8	Κυκλική οικονομία / υποβολή δεδομένων IoT	61
7.9	Ασφαλής Διαχείριση Υλικολογισμικού	61
7.10	Συγκριτική αξιολόγηση περιπτώσεων χρήσης	62
Κεφάλαιο 8ο: Προτεινόμενο πλαίσιο Επιλογής Αρχιτεκτονικής Shimmer		64
8.1	Σκοπός της προτεινόμενης προσέγγισης	64
8.2	Βασικές απαιτήσεις εφαρμογών	64
8.3	Προτεινόμενα αρχιτεκτονικά πρότυπα	65
8.3.1	Πρότυπο Α: Άμεση καταγραφή το Layer 1	65
8.3.2	Πρότυπο Β: Gateway-assisted αρχιτεκτονική	66
8.3.3	Πρότυπο Γ: Υβριδική αρχιτεκτονική προστασίας ιδιωτικότητας	66
8.3.4	Πρότυπο Δ: Smart-contract και Layer 2 αρχιτεκτονική	66
8.4	Προτεινόμενη διαδικασία λήψης απόφασης για την επιλογή αρχιτεκτονικής	67
8.5	Πίνακας αντιστοίχισης απαιτήσεων και αρχιτεκτονικής	67
8.6	Ποιοτική αξιολόγηση του προτεινόμενου πλαισίου	68
8.7	Συμβολή του προτεινόμενου πλαισίου	69
8.8	Περιορισμοί και μελλοντική επέκταση	69
Κεφάλαιο 9ο: Συμπεράσματα		70
ΒΙΒΛΙΟΓΡΑΦΙΑ		71
ΠΑΡΑΡΤΗΜΑ Α : ΤΙΤΛΟΣ ΠΑΡΑΡΤΗΜΑΤΟΣ		75

Κατάλογος Σχημάτων

Σχήμα 4.1: Η δομή του blockchain	21
Σχήμα 4.2α : Αρχιτεκτονική του blockchain	22
Σχήμα 4.2β : Blockchain και blockDAG	24
Σχήμα 4.3: Παράδειγμα ενός IOTA Tangle	28
Σχήμα 4.4 : Δισδιάστατη Δομή που βασίζεται σε DAG	28
Σχήμα 4.5: Απεικόνιση της ενσωμάτωσης του ROS2 με το πλέγμα IOTA (επίπεδο 1) και τα έξυπνα συμβόλαια IOTA	29
Σχήμα 4.6: Αρχιτεκτονική συστήματος υψηλού επιπέδου	32
Σχήμα 4.7:Σύστημα που βασίζεται σε IOTA για SDN	33
Σχήμα 4.8: Απεικόνιση τοπολογίας Tangle και τοπολογίας blockchain	35
Σχήμα 4.9: Απεικόνιση παραδοσιακού blockchain, του IOTA Tangle και της αρχιτεκτονικής ISCP δύο επιπέδων	36
Σχήμα 5.1: Παράδειγμα διαδικασίας συναίνεσης στο Tangle	43
Σχήμα 5.2: Ταξινόμηση μηχανισμών συναίνεσης	46
Σχήμα 5.3: Η μεγαλύτερη αλυσίδα σε PoW έναντι του βαρύτερου DAG στο Tangle	47
Σχήμα 6.1: Ανάλυση απειλών ασφαλείας και ευπαθειών στο SDN ανά επίπεδο	49
Σχήμα 7.1: Δείγμα διαδικασίας PowerGraph	55

Κατάλογος Πινάκων

Πίνακας 3.1: Πίνακας βιβλιογραφικής αναζήτησης	19
Πίνακας 4.1:Βασικές διαφορές μεταξύ του παλαιού IOTA και του IOTA 2.0	33
Πίνακας 4.2:Συγκριτική ανάλυση τεχνολογιών Blockchain και DAG	34
Πίνακας 4.3:Σύγκριση Blockchain και DAG-based DLT	35
Πίνακας 5.1:Σύγκριση μηχανισμών συναίνεσης	47
Πίνακας 8.5:Πίνακας αντιστοίχισης απαιτήσεων και αρχιτεκτονικής	67

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ABAC - Attribute-Based Access Control

API - Διεπαφή Προγραμματισμού Εφαρμογών (Application Programming Interface)

BFT - Βυζαντινή Ανοχή Σφάλματος / Βυζαντινή Συναίνεση σε Σφάλματα (Byzantine Fault Tolerance)

CapBAC - Capability-Based Access Control

CAS - Συνδεδεμένα Αυτόνομα Συστήματα (Connected Autonomous Systems)

CFT - Ανοχή σφάλματος κατάρρευσης (Crash Fault Tolerance)

CP-ABE - Κρυπτογράφηση βασισμένη σε χαρακτηριστικά με πολιτική κρυπτογραφημένου κειμένου (Ciphertext-Policy Attribute-Based Encryption)

DAG - Κατευθυνόμενο Ακυκλικό Γράφημα (Directed Acyclic Graph)

DCACI - Πλαίσιο ελέγχου πρόσβασης βασισμένο σε αποκεντρωμένες δυνατότητες χρησιμοποιώντας IOTA (Decentralized Capabilities-based Access Control framework using IOTA)

DCE - Ψηφιακή Κυκλική Οικονομία (Digital Circular Economy)

DLT - Τεχνολογία Κατανεμημένου Καθολικού (Distributed Ledger Technology)

DoS / DDoS - Άρνηση υπηρεσίας / Κατανεμημένη άρνηση υπηρεσίας (Denial of Service / Distributed Denial of Service)

DTLS - Ασφάλεια Επιπέδου Μεταφοράς Datagram (Datagram Transport Layer Security)

EBC - Ηλεκτρονικός Κώδικας Προϊόντος (Electronic Product Code)

EE / VE - Εικονικές Επιχειρήσεις (Virtual Enterprises)

EVM - Εικονική Μηχανή Ethereum (Ethereum Virtual Machine)

FPC - Γρήγορη Πιθανοτική Συναίνεση (Fast Probabilistic Consensus)

FPC-BI - Γρήγορη Πιθανοτική Συναίνεση εντός Βυζαντινών Υποδομών (Fast Probabilistic Consensus within Byzantine Infrastructures)

HIE - Ανταλλαγή Πληροφοριών Υγείας (Health Information Exchange)

IoT - Διαδίκτυο των Πραγμάτων (Internet of Things)

IPFS - Διαπλανητικό Σύστημα Αρχείων (Inter-Planetary File System)

ISP - Πάροχοι Υπηρεσιών Διαδικτύου (Internet Service Providers)

L1 - Επίπεδο 1 (Layer 1)

L2 - Επίπεδο 2 (Layer 2)

MAM - Ανταλλαγή μηνυμάτων με μάσκα και έλεγχο ταυτότητας (Masked Authenticated Messaging)

MCMC - Αλυσίδα Markov Monte Carlo (Markov Chain Monte Carlo)

OTV - On Tangle Voting

P2P - Ομότιμο δίκτυο (Peer-to-peer)

PBFT - Πρακτική Βυζαντινή Ανοχή Σφαλμάτων (Practical Byzantine Fault Tolerance)

PoS - Απόδειξη Συμμετοχής (Proof of Stake)

PoW - Απόδειξη Εργασίας (Proof of Work)

PoX - Απόδειξη X (Proof of X)

RFID - Αναγνώριση Ραδιοσυχνοτήτων (Radio Frequency Identification)

SDK - Κιτ ανάπτυξης λογισμικού (Software Development Kit)

SLA - Συμφωνία Επιπέδου Υπηρεσιών (Service Level Agreement)

SLR - Συστηματική Βιβλιογραφική Επισκόπηση (Systematic Literature Review)

SMR - Αναπαραγωγή Μηχανής Κατάστασης (State Machine Replication)

SRRS - Synchronised Random Reality Selection (Συγχρονισμένη Τυχαία Επιλογή Πραγματικότητας)

TLS - Ασφάλεια Επιπέδου Μεταφοράς (Transport Layer Security)

TPS - Συναλλαγές ανά δευτερόλεπτο (Transactions Per Second)

URTS - Ομοιόμορφη Επιλογή Τυχαίων Συμβουλών (Uniform Random Tip Selection)

URW - Μη Βαρυμένη Τυχαία Εργασία (Unweighted Random Walk)

UTXO - Αδιάθετη Έξοδος Συναλλαγών (Unspent Transaction Output)

VR - Αναπαραγωγή με σήμανση Views (Viewstamped Replication)

WRW - Βαρυμένη Τυχαία Εργασία (Weighted Random Walk)

Κεφάλαιο 1ο: Εισαγωγή

Ο τρόπος ζωής των ανθρώπων στην εποχή μας, εξαρτάται όλο και περισσότερο από τις πολυάριθμες ηλεκτρονικές συσκευές. Τα ασύρματα δίκτυα αισθητήρων έχουν γίνει ολοένα και πιο κοινά σε καθημερινές εφαρμογές, λόγω της μείωσης του κόστους της τεχνολογίας και της βελτιωμένης απόδοσης, της ανθεκτικότητας και της επεκτασιμότητας των προϊόντων. Για να συνδεθεί η πληθώρα των έξυπνων συσκευών και να καταστεί δυνατή η επικοινωνία μεταξύ τους, είναι απαραίτητες νέες δικτυακές αρχιτεκτονικές επικοινωνίας. Το IOTA, που είναι μια σχετικά νέα τεχνολογία και αρκετά ανεξερεύνητη, επιτρέπει ακριβώς αυτό (Ahuja, et al. 2016).

Το IOTA είναι ένα κρυπτονόμισμα που εμφανίστηκε στα τέλη του 2015 και στοχεύει στην αντιμετώπιση των κύριων προβλημάτων του Blockchain. Το IOTA προσφέρει μια εντελώς νέα τεχνολογία, η οποία εξακολουθεί να είναι αποκεντρωμένη αλλά μπορεί επίσης να επεξεργαστεί έναν μεγάλο αριθμό συναλλαγών. Η έννοια της Τεχνολογίας Κατανεμημένου Καθολικού (DLT) επέκτεινε την έννοια του blockchain, η οποία κάλυπτε τόσο τις αμετάβλητες βάσεις δεδομένων που βασίζονται σε αλυσίδες όσο και σε Κατευθυνόμενα Ακυκλικά Γραφήματα (DAG) και διατηρούνται από πολλαπλούς συμμετέχοντες. Ένας μεγάλος αριθμός δομών δεδομένων έχει προταθεί σε DLT, για την κάλυψη διαφορετικών απαιτήσεων εφαρμογών. Αυτή η τεχνολογία ονομάζεται Tangle, ένα άλλο είδος βάσης δεδομένων. Με αυτόν τον αλγόριθμο, το IOTA μπορεί θεωρητικά να επεξεργαστεί έναν μεγάλο αριθμό συναλλαγών και να αυξήσει τη συνολική υπολογιστική και συναλλακτική ικανότητα του δικτύου του, εάν συμμετέχουν περισσότεροι συμμετέχοντες. Από την εισαγωγή του πρώτου κρυπτονομίσματος, του Bitcoin, το 2008, η αύξηση της δημοτικότητας των τεχνολογιών κατανεμημένου καθολικού (DLT) έχει οδηγήσει σε αυξανόμενη ζήτηση και, κατά συνέπεια, σε μεγαλύτερο αριθμό συμμετεχόντων στο δίκτυο γενικά. Η κλιμάκωση λύσεων που βασίζονται σε blockchain για την αντιμετώπιση αρκετών χιλιάδων συναλλαγών ανά δευτερόλεπτο, ή με έναν αυξανόμενο αριθμό κόμβων, ήταν πάντα ένας επιθυμητός στόχος για τους περισσότερους προγραμματιστές (Kahmann 2023), και έχουν προκαλέσει μεγάλο ενδιαφέρον στον ακαδημαϊκό χώρο, στη βιομηχανία, στον χρηματοπιστωτικό κλάδο και την κοινωνία στο σύνολό της.

Το Blockchain θεωρείται ως ένα πλήρως αποκεντρωμένο σύστημα και μια τεχνολογία ασφαλούς σχεδιασμού. Το ίδιο το blockchain είναι μια βάση δεδομένων που παρακολουθεί όλες τις συναλλαγές που πραγματοποιούνται στο δίκτυο και αναπαράγεται σε κάθε συμμετέχοντα κόμβο. Ουσιαστικά, υλοποιεί ένα κατανεμημένο καθολικό, χωρίς να βασίζεται σε μια κεντρική αρχή για την ενίσχυση της εμπιστοσύνης μεταξύ των συμμετεχόντων ή για την εκκαθάριση των συναλλαγών (Xiao et al. 2020). Μεταξύ διαφόρων βασικών συνιστωσών, το πρωτόκολλο συναίνεσης είναι η καθοριστική τεχνολογία πίσω από την ασφάλεια και την απόδοση του blockchain (Xiao et al. 2020). Το Shimmer Network είναι ένα πειραματικό blockchain δίκτυο (DLT) που ανήκει στο οικοσύστημα του IOTA. Το Shimmer Network παρέχει στο πρωτόκολλο IOTA την απαραίτητη βάση για την εκκίνηση έξυπνων συμβολαίων πολλαπλών αλυσίδων σχεδόν χωρίς κανένα σφάλμα. Το Shimmer είναι ένα “δοκιμαστικό περιβάλλον” όπου δοκιμάζονται νέες τεχνολογίες πριν μπουν στο κανονικό δίκτυο (IOTA). Σε αντίθεση με τα κλασικά blockchain (π.χ. Bitcoin), το Shimmer δεν χρησιμοποιεί blocks αλλά DAG (Directed Acyclic Graph Κατευθυνόμενα Ακυκλικά Γραφήματα). Το Shimmer network είναι το δίκτυο σταδιοποίησης για το κύριο δίκτυο IOTA. Εκεί οι νέες αλλαγές πρωτοκόλλου υποβάλλονται σε αξιολόγηση για λειτουργικότητα, επεκτασιμότητα και ασφάλεια πριν εφαρμοστούν στο κύριο δίκτυο IOTA. Το Shimmer διακρίνεται από τα τυπικά δίκτυα δοκιμών επειδή διαθέτει ένα διακριτικό που ονομάζεται SMR, το οποίο διαπραγματεύεται ενεργά σε μεγάλα χρηματιστήρια. Αυτό το χαρακτηριστικό προσδίδει πραγματική χρηματική αξία στο δίκτυο, ενισχύοντας το κίνητρο για τη δοκιμή επερχόμενων αλλαγών πρωτοκόλλου.

Η ραγδαία ανάπτυξη του Διαδικτύου των Πραγμάτων (IoT) υποστηρίζει τη δυνατότητα διαφόρων βιομηχανικών τομέων, να προχωρήσουν προς την ψηφιοποίηση τους και την ανάπτυξη τεχνητής νοημοσύνης. Η μεγαλύτερη διασύνδεση δεδομένων, οι αισθητήρες και τα δίκτυα ανοίγουν πολλές συναλλαγές δεδομένων (Rochman et al. 2022).

Παρά την αρκετά μεγάλη έρευνα που έχει διεξαχθεί, όσον αφορά τα blockchain και τα DAG-based DLT συστήματα, για την αρχιτεκτονική και τους μηχανισμούς συναίνεσης του Shimmer Network, δεν υπάρχουν αρκετές εργασίες δημοσιευμένες στη βιβλιογραφία. Η παρούσα εργασία στοχεύει να παράσχει μια ολοκληρωμένη εικόνα για τις τρέχουσες προσεγγίσεις που αφορούν την αρχιτεκτονική των DAG-based DLT συστημάτων και τους μηχανισμούς Συναίνεσης του Shimmer Network. Επιπλέον, θέτει την ερευνητική ατζέντα σχετικά με την επεκτασιμότητα, την ασφάλεια και τη λειτουργία μηχανισμών συναίνεσης σε περιβάλλοντα DAG, λαμβάνοντας υπόψη μια ανασκόπηση μελετών περίπτωσης χρήσης τους. Η παρούσα εργασία βασίζεται σε συστηματική βιβλιογραφική επισκόπηση (Systematic Literature Review - SLR), με στόχο τη ενδελεχή ανάλυση της αρχιτεκτονικής και των μηχανισμών συναίνεσης του Shimmer Network.

Η δομή της παρούσας εργασίας είναι η εξής: Η Ενότητα 2 ξεκινά με το βασικό υπόβαθρο που σχετίζεται με το Shimmer network. Η Ενότητα 3 περιγράφει τη μεθοδολογία συστηματικής ανασκόπησης της βιβλιογραφίας, θέτοντας τα ερωτήματα για αυτήν την εργασία. Στην ενότητα 4 διερευνάται και παρουσιάζεται η αρχιτεκτονική των DAG-based DLT συστημάτων όπως το IOTA και το Shimmer. Η Ενότητα 5 παρουσιάζει τη βιβλιογραφία που σχετίζεται με τον τρόπο λειτουργίας των μηχανισμών συναίνεσης σε DAG δίκτυα. Στην ενότητα 6 παρέχεται μια συζήτηση που απαντά στα ερωτήματα ποιες είναι οι βασικές προκλήσεις (ασφάλεια, επεκτασιμότητα, ιδιωτικότητα), ενώ η ενότητα 7 αναφέρεται στις βασικές εφαρμογές και χρήσεις των DAG-based DLT. Στην Ενότητα 8 προτείνεται ένα πλαίσιο Επιλογής Αρχιτεκτονικής Shimmer/IOTA για εφαρμογές IoT, ενώ στην Ενότητα 9 ολοκληρώνεται η εργασία με συμπεράσματα και προοπτικές.

Κεφάλαιο 2ο: Βασικό Υπόβαθρο του IOTA και του Shimmer network

Το IOTA (γνωστό και ως κατανεμημένο καθολικό (Poron, 2017)) είναι ένα κρυπτονόμισμα που εμφανίστηκε στα τέλη του 2015 και στοχεύει στην αντιμετώπιση των κύριων προβλημάτων του Blockchain. Οι τεχνολογίες Blockchain, όπως το Bitcoin, αντιμετωπίζουν διάφορα συστημικά προβλήματα, όπως η συμφόρηση δικτύου. Με λίγα λόγια, δεν μπορούν να επεκταθούν περαιτέρω και δεν είναι σε θέση να επεξεργαστούν περισσότερες συναλλαγές, από το όριο των επτά ανά δευτερόλεπτο. Το IOTA αντιμετωπίζει αυτά τα ζητήματα και προσφέρει μια εντελώς νέα τεχνολογία, η οποία στοχεύει σε υψηλότερο βαθμό αποκέντρωσης, αλλά παράλληλα μπορεί να χαρακτηριστεί και από υψηλή επεκτασιμότητα (Alexander 2018). Η τεχνολογία IOTA μπορεί να ξεπεράσει τους πρακτικούς περιορισμούς του κλασικού Blockchain, ενώ συζητείται η εφαρμογή του IOTA για την ασφαλή μεταφορά δεδομένων αισθητήρων IoT. Το IOTA Tangle αναπτύχθηκε για να αντιμετωπίσει τις απαιτήσεις των εφαρμογών IoT, όπως η ιδιωτικότητα και η ασφάλεια.

Το IOTA είναι μια αναδυόμενη πλατφόρμα, που έχει σχεδιαστεί ειδικά για το διαδίκτυο των πραγμάτων, ώστε να ξεπεραστούν τα προβλήματα της επεκτασιμότητας, των τελών συναλλαγών και της εξόρυξης, η οποία θεωρείται ως μια εργασία εκτεταμένων πόρων, που δεν διαθέτουν άλλα κρυπτονομίσματα, χρησιμοποιώντας την τεχνολογία blockchain (Nakamoto et al., 2008). Το κύριο συστατικό του IOTA είναι το Tangle το οποίο βασίζεται στην έννοια ενός Κατευθυνόμενου Ακυκλικού Γραφήματος (DAG), το οποίο θεωρείται το ημερολόγιο (ledger) που αποθηκεύει συναλλαγές (Poron, 2017). DAG δηλαδή Directed Acyclic Graph Directed σημαίνει ότι κάθε γραμμή ή βέλος δείχνει αυστηρά από έναν κόμβο σε έναν άλλο, παρέχοντας μια σαφή μονόδρομη διαδρομή ή εξάρτηση Directed). Το σύστημα περιέχει μηδενικούς βρόχους ή κλειστά κυκλώματα, που σημαίνει ότι δεν μπορεί ποτέ να γίνει μετακίνηση προς τα εμπρός κατά μήκος των βελών και να επιστρέψετε στον αρχικό κόμβο, και τέλος είναι μια συλλογή σημείων σύνδεσης (κορυφές/κόμβοι) που συνδέονται μεταξύ τους για να χαρτογραφήσουν σχέσεις (Graph).

Το Tangle είναι το πρωτόκολλο ή η δομή δεδομένων, μια συλλογή από κόμβους και βέλη, που χρησιμοποιείται στο IOTA για την αποθήκευση των συναλλαγών. Το tangle είναι ένα άλλο είδος βάσης δεδομένων, όπου αποθηκεύονται όλες οι συναλλαγές που πραγματοποιούνται μέσω του συστήματος, που μοιράζονται οι χρήστες. Με αυτόν τον αλγόριθμο, το IOTA μπορεί θεωρητικά να επεξεργαστεί έναν μεγάλο αριθμό συναλλαγών και να αυξήσει τη δύναμη του δικτύου του. Όλες οι κορυφές ή οι κόμβοι που περιέχουν δεδομένα (συναλλαγές) συνδέονται μεταξύ τους μέσω ακμών. Οι ακμές που ονομάζονται Γονικές είναι τουλάχιστον δύο, μπορεί όμως να είναι και πολύ περισσότερες. Εάν υπάρχει μια τοποθεσία με λιγότερες από δύο ακμές, αυτό σημαίνει ότι πρόκειται για μη επιβεβαιωμένες συναλλαγές (Alsboui et al., 2019).

Σε αντίθεση με τα παραδοσιακά blockchains, με δομή DAG, το IOTA έχει συναλλαγές χωρίς κόστος και είναι πιο αποκεντρωμένο, καθιστώντας το ταχύτερο από τα παραδοσιακά blockchains και με μεγαλύτερη δυνατότητα επεκτασιμότητας. Ένα tangle μπορεί να αποτελείται από λίγες κορυφές και κατευθυνόμενες ακμές. Κάθε κόμβος αντιπροσωπεύει μια συναλλαγή, η κεφαλή της κατευθυνόμενης ακμής αντιπροσωπεύει μια επαληθευμένη συναλλαγή και η ουρά αντιπροσωπεύει έναν εκτελεστή επαλήθευσης (Rochman et al., 2022).

Το IOTA Tangle χρησιμοποιεί μια δομή άμεσου ακυκλικού γραφήματος (DAG) για το καθολικό, με το πρωτόκολλό του να προσφέρει χαρακτηριστικά ελκυστικά για τον τομέα του IoT, σε σχέση με τις περισσότερες εναλλακτικές λύσεις blockchain, όπως ανέπαφες συναλλαγές, υψηλότερες εφικτές συναλλαγές ανά δευτερόλεπτο (TPS) και χαμηλότερη κατανάλωση ενέργειας. Λόγω της εσωτερικής, παράλληλα προσανατολισμένης δομής δεδομένων τους, οι λύσεις που βασίζονται σε DAG προσφέρουν σημαντικά υψηλότερη απόδοση συναλλαγών, σε σύγκριση με τις πλατφόρμες που βασίζονται σε blockchain. Ωστόσο, λόγω της σχετικά πρώιμης φάσης ωριμότητάς τους, οι πλατφόρμες που βασίζονται πλήρως σε DAG πρέπει να εξελιχθούν περαιτέρω, όσον αφορά το σύνολο χαρακτηριστικών τους για να επιτύχουν το ίδιο επίπεδο προγραμματισμού και εξάπλωσης με τις σύγχρονες πλατφόρμες blockchain (Kahmann 2023). Η αρχική υλοποίηση του IOTA βασιζόταν σε μια κεντρική λύση συντονιστή bootstrap για συναίνεση, η οποία περιόριζε τον βαθμό αποκέντρωσης

και επεκτασιμότητας. Αυτός ο περιορισμός, μαζί με άλλους, αντιμετωπίζονται με την κυκλοφορία του IOTA 2.0. (Alsboui et al., 2023)

Η Τεχνολογία Κατανεμημένου Καθολικού (DLT) είναι μια αναδυόμενη εξέλιξη που μοιράζεται δεδομένα μεταξύ διαφορετικών συμμετεχόντων, που αναπτύσσονται σε διάφορες τοποθεσίες σε όλο τον κόσμο. Αυτή η τεχνολογία παρέχει πολλά οφέλη σε διάφορες εφαρμογές IoT. Η βιβλιογραφία αποκαλύπτει ένα αυξανόμενο ενδιαφέρον της σχετικής ερευνητικής κοινότητας για την DLT, θεωρώντας την ως μια πιθανή λύση για την αντιμετώπιση ορισμένων από τις προκλήσεις που σχετίζονται με το IoT, όπως η επεκτασιμότητα, ο έλεγχος πρόσβασης, η ασφάλεια και η ιδιωτικότητα. (Alsboui et al., 2020a, Fan et al., 2019, Alsboui et al., 2023). Η έννοια του πλήρους κόμβου IOTA (Foundation, 2016), ο οποίος μπορεί να οριστεί ως κόμβος εντός της αρχιτεκτονικής tangle είναι ικανός να βρίσκει γείτονες και να επικοινωνεί μαζί τους, να συνδέει δεδομένα στο tangle, να ομαδοποιεί και να υπογράφει, να επιλέγει συμβουλές, να επικυρώνει, PoW (Απόδειξη Εργασίας) και να συνδέει δεδομένα στο tangle. Οι πλήρεις κόμβοι IOTA έχουν υψηλή υπολογιστική ικανότητα και είναι υπεύθυνοι για την εκτέλεση του PoW εκ μέρους των τελικών κόμβων, λαμβάνοντας υπόψη ότι οι τελικοί κόμβοι έχουν περιορισμένους πόρους. Για να εκδοθεί μια συναλλαγή από έναν κόμβο, ο κόμβος θα πρέπει να εργαστεί για να εγκρίνει δύο προηγούμενες συναλλαγές. Η επιλογή των δύο προηγούμενων συναλλαγών γίνεται χρησιμοποιώντας την τεχνική επιλογής συμβουλών, όπου η προεπιλογή είναι η τεχνική Markov Chain Monte Carlo (MCMC) (Poron, 2017). Ο κύριος στόχος του δικτύου Tangle είναι να κάνει όλες τις συναλλαγές να επιβεβαιωθούν και να μετατρέψει όλες τις μη επιβεβαιωμένες συναλλαγές σε επιβεβαιωμένες συναλλαγές. Η τεχνική MCMC εκτελείται η φορές. Το Genesis είναι η πρώτη συναλλαγή του δικτύου, η οποία εγκρίνεται άμεσα ή έμμεσα από τις άλλες συναλλαγές. Το IOTA Tangle έχει σχεδιαστεί με τρόπο που να επιτρέπει την πιο επεκτάσιμη διευθέτηση συναλλαγών, με αποτέλεσμα οι συναλλαγές να γίνονται πιο ασφαλείς και αποτελεσματικές (Poron, 2017).

Η Τεχνολογία Κατανεμημένου Καθολικού (DLT) έχει καταστεί θεμελιώδης στην υποστήριξη ασφαλών και διαφανών συστημάτων συναλλαγών σε αποκεντρωμένα δίκτυα. Διατηρώντας ένα αμετάβλητο και μόνο για προσάρτηση καθολικό, το DLT επιτρέπει ένα περιβάλλον χωρίς εμπιστοσύνη, όπου οι συμμετέχοντες μπορούν να πραγματοποιούν συναλλαγές απευθείας χωρίς μεσάζοντες. Αυτή η τεχνολογία, ιδιαίτερα η εφαρμογή της σε κρυπτονομίσματα όπως το Bitcoin και το Ethereum, έχει προσελκύσει μεγάλο ενδιαφέρον λόγω των δυνατοτήτων της για βελτιωμένη διαφάνεια, λειτουργική αποδοτικότητα και αποκέντρωση (Raikwar et al 2025).

Τα πρωτόκολλα που βασίζονται σε DAG διαφέρουν από τα παραδοσιακά DLT στον τρόπο που δημιουργούν και αναπαριστούν γνώση σχετικά με τις συναλλαγές και τις σχέσεις μεταξύ τους. Ενώ τα παραδοσιακά DLT έχουν απλή ομοιογενή σημασιολογία συνδεδεμένη με μπλοκ και συνδέσμους μεταξύ των μπλοκ, η σημασιολογία των κορυφών και των ακμών στα πρωτόκολλα που βασίζονται σε DAG είναι λεπτή και ποικίλη. Για παράδειγμα, τα Vite και Jointgraph έχουν κορυφές στιγμιότυπων που μπορούν να χρησιμοποιηθούν για τον συγχρονισμό των καταστάσεων του ledger των συμμετεχόντων κόμβων. Τα Byteball και Jh-DAG προσθέτουν κορυφές ψήφου για να επιτύχουν συναίνεση επιλέγοντας μια κύρια αλυσίδα. Παρ' όλα αυτά, η δημιουργία τέτοιων κορυφών στιγμιότυπων ή ψήφου μπορεί είτε να απαιτεί συναίνεση από τους συμμετέχοντες κόμβους, είτε να απαιτεί ειδικούς κόμβους. Αυτό παρουσιάζει ένα συμβιβασμό στην αξιοποίηση τέτοιων κορυφών στο DLT. Ένα άλλο παράδειγμα είναι η λεπτομέρεια και η μέθοδος επίλυσης συγκρούσεων (Raikwar et al 2025). Η λεπτομερής επίλυση των συγκρούσεων επιτρέπει μεγαλύτερη ευελιξία και ενδεχομένως ταχύτερη οριστικοποίηση των συναλλαγών, ωστόσο επιβάλλει μεγαλύτερη επιβάρυνση και ανάλογα με τη μέθοδο, μπορεί να καθυστερήσει τη δημιουργία νέων κορυφών. Η οικοδόμηση γνώσης είναι σημαντική στα DLT που βασίζονται σε DAG, επειδή έχει σημαντικό αντίκτυπο στο μέγεθος του DAG, τον ρυθμό με τον οποίο προστίθενται νέες συναλλαγές, την οριστικοποίηση των συναλλαγών και ούτω καθεξής. Επιπλέον, η κατανόηση αυτών των διαστάσεων οικοδόμησης γνώσης είναι ζωτικής σημασίας για την αξιοποίηση του πλήρους δυναμικού των DLT που βασίζονται σε DAG σε πρακτικές εφαρμογές. Οι βιομηχανίες και οι προγραμματιστές χρειάζονται ένα πλαίσιο για να αξιολογήσουν ποια DLT που βασίζεται σε DAG και ποιες διαστάσεις οικοδόμησης γνώσης ταιριάζουν καλύτερα στις ανάγκες τους, λαμβάνοντας υπόψη παράγοντες, όπως η απόδοση συναλλαγών, η συνέπεια των δεδομένων και η ανταλλαγή αποκέντρωσης-ασφάλειας (Raikwar et al 2025).

Το [Shimmer Network](#) είναι ένα αποκεντρωμένο, γρήγορο και χωρίς χρεώσεις (feeless) δίκτυο στρώματος 1 (L1), το οποίο λειτουργεί ως το επίσημο δίκτυο δοκιμών και επικύρωσης του πρωτοκόλλου IOTA. Χρησιμοποιεί τεχνολογία κατευθυνόμενου άκυκλου γράφου (DAG) και υποστηρίζει έξυπνα συμβόλαια μέσω του ShimmerEVM. Το Shimmer είναι ένα άψογο, παράλληλο επίπεδο υποδομής DAG για την απρόσκοπτη σύνδεση έξυπνων αλυσίδων συμβολαίων. Με το εκτεταμένο καθολικό UTXO και τις μοναδικές δυνατότητες tokenization, το Shimmer προσφέρει πρωτοφανή διαλειτουργικότητα και δυνατότητα σύνθεσης μεταξύ blockchain, ενώ παράλληλα επιτρέπει την πλήρη προσαρμογή τους. Χωρίς να δεσμεύεται από δαπανηρές, αναξιόπιστες γέφυρες από το ένα δίκτυο στο άλλο, το Shimmer ανοίγει άπειρες ευκαιρίες συναλλαγών μεταξύ αλυσίδων.

Προς το παρόν, το Shimmer λειτουργεί χρησιμοποιώντας την έκδοση πρωτοκόλλου Stardust, που αποτελεί σημαντική εξέλιξη της αρχιτεκτονικής του Shimmer/IOTA οικοσυστήματος, καθώς εισάγει βελτιωμένους μηχανισμούς διαχείρισης assets και αποδοτικότερη λειτουργία του Tangle, διευκολύνοντας έτσι την δημιουργία διακριτικών και την ενσωμάτωση αλυσίδων έξυπνων συμβολαίων L2 στο L1. Επιπλέον, το Shimmer είναι το καθορισμένο δίκτυο για το Shimmer EVM, μια λύση Layer 2 που επιτρέπει τον προγραμματισμό έξυπνων συμβολαίων πάνω από το θεμελιώδες επίπεδο (Cech 2020).

Το ShimmerEVM είναι ένα blockchain που βασίζεται σε Directed Acyclic Graph (DAG) για να διασφαλίσει τη ανεξαρτησία και την αμετάβλητη φύση των δεδομένων. Το ShimmerEVM διευκολύνει την εκτέλεση έξυπνων συμβολαίων, προσφέροντας ένα αποκεντρωμένο, διαφανές και ασφαλές περιβάλλον χωρίς να βασίζεται στην παραδοσιακή τεχνολογία blockchain. Το επίκεντρο αυτού του συστήματος είναι η εφαρμογή έξυπνων συμβολαίων με επίκεντρο την ασφάλεια (Maliki et al. 2024).

Η μελέτη των Nzakuna et al. (2024) είναι η πρώτη που ρίχνει φως στα χαρακτηριστικά του πραγματικού Tangle στο στάδιο Stardust, τα οποία είναι ιδιαίτερα χρήσιμα για την κατανόηση της εξέλιξης του ledger και συμβάλλουν στις βελτιώσεις του. Οι ερευνητές αυτοί διαπίστωσαν ότι η επιβεβαίωση νέων μπλοκ είναι δύο φορές ταχύτερη στο στάδιο Stardust και το Tangle χρησιμοποιείται μέχρι τώρα πολύ κάτω από την ικανότητά του να μεταφέρει και να ασφαλίζει δεδομένα από συσκευές IoT.

Κεφάλαιο 3ο: Μεθοδολογία συστηματικής βιβλιογραφικής ανασκόπησης

Η παρούσα εργασία ακολουθεί τη μεθοδολογία της Συστηματικής Βιβλιογραφικής Ανασκόπησης (Systematic Literature Review – SLR), με σκοπό τη συστηματική διερεύνηση της αρχιτεκτονικής και των μηχανισμών συναίνεσης του Shimmer Network και των DAG-based Distributed Ledger Technologies. Η ερευνητική μέθοδος που χρησιμοποιήθηκε για τη διεξαγωγή της ανασκόπησης βασίστηκε στην εξέταση επιστημονικών εργασιών καταχωρημένων στις βάσεις δεδομένων Scopus και Google Scholar, τα οποία δημοσιεύθηκαν κατά την τελευταία δεκαπενταετία.

Στόχος ήταν να καλυφθεί ένα ευρύ φάσμα θεμάτων σχετικά με την αρχιτεκτονική των DAG-based DLT συστημάτων (IOTA και Shimmer), τον τρόπο λειτουργίας των μηχανισμών συναίνεσης σε DAG δίκτυα και τις βασικές προκλήσεις (ασφάλεια, επεκτασιμότητα, ιδιωτικότητα). Το πλαίσιο PRISMA 2020 καθοδήγησε τη συστηματική διαδικασία που ακολουθήθηκε για τον εντοπισμό και την επιλογή της βιβλιογραφίας.

Η ανάλυση πρώτου επιπέδου επικεντρώθηκε στην περιγραφική εξέταση της επιλεγμένης βιβλιογραφίας μετά τη διαδικασία επιλογής μελετών. Η ανάλυση περιελάμβανε την ταξινόμηση των μελετών ανάλογα με το έτος δημοσίευσης, τον τύπο δημοσίευσης, την πηγή βάσης δεδομένων και το ερευνητικό επίκεντρο. Επιπλέον, διπλότυπα αρχεία που εντοπίστηκαν σε πολλαπλές βάσεις δεδομένων αφαιρέθηκαν πριν από την ανάλυση για να διασφαλιστεί η αξιοπιστία του τελικού συνόλου δεδομένων. Σκοπός της ανάλυσης πρώτου επιπέδου ήταν να δημιουργηθεί μια ολοκληρωμένη επισκόπηση της υπάρχουσας βιβλιογραφίας σχετικά με την αρχιτεκτονική και τους μηχανισμούς συναίνεσης του Shimmer Network και των DAG-based Distributed Ledger Technologies. Τα αποτελέσματα αυτής της ανάλυσης χρησιμοποιήθηκαν για να περιγράψουν την εξέλιξη της ερευνητικής δραστηριότητας και να υποστηρίξουν την επακόλουθη θεματική ανάλυση των επιλεγμένων δημοσιεύσεων.

Η σχετική βιβλιογραφία αποκτήθηκε από τις ηλεκτρονικές βάσεις δεδομένων ACM Digital Library, IEEE Xplore, Web of Science, Scopus, ScienceDirect, Google Scholar. Η αναζήτηση αφορούσε δημοσιεύσεις εντός του χρονικού διαστήματος 2010 έως 2026. Η αναζήτηση εργασιών δομήθηκε σε δύο φάσεις, χρησιμοποιώντας διαφορετικά σύνολα λέξεων-κλειδιών. Τέθηκαν τα εξής ερωτήματα: (1) Ποια είναι η αρχιτεκτονική των DAG-based DLT συστημάτων όπως το IOTA και το Shimmer (2) Πώς λειτουργούν οι μηχανισμοί συναίνεσης σε DAG δίκτυα (3) Ποιες είναι οι βασικές προκλήσεις (ασφάλεια, επεκτασιμότητα, ιδιωτικότητα) (4) Ποιες είναι οι βασικές εφαρμογές των DAG-based DLT.

Για να καλύψουμε ένα ευρύ σύνολο δημοσιεύσεων, ετέθησαν οι λέξεις-κλειδιά «IOTA», "Shimmer Network", "Directed Acyclic Graph" "DAG DLT" "consensus mechanism" "scalability", "security" και σε δεύτερο στάδιο συνδυασμός των λέξεων αυτών (1."Shimmer Network" και architecture or protocol ,2. "Shimmer Network" or ShimmerEVM and application or "use case" 3. Shimmer or IOTA and architecture or scalability, 4. "IOTA" or "Shimmer Network" and consensus , 5: "IOTA" or "Shimmer" and security or architecture, 6: "IOTA Tangle" OR "Shimmer DLT"and IoT OR "Internet of Things" 7:"DAG-based DLT" or "DAG-based blockchain" and security or scalability or privacy κ.ά.

Η αρχική αναζήτηση στη βάση δεδομένων εμφάνισε 103700 άρθρα. Για να εντοπίσουμε και να φιλτράρουμε τα άρθρα, ελέγξαμε πρώτα τη συνάφεια κάθε άρθρου αναλύοντας τον τίτλο, την περίληψη και τις λέξεις-κλειδιά. Ως κριτήρια ένταξης χρησιμοποιήθηκαν: Επιστημονικά άρθρα με

διαδικασία αξιολόγησης από reviewers Δημοσιεύσεις στην αγγλική γλώσσα σχετικές με αρχιτεκτονικές DAG, IOTA, Shimmer και μηχανισμούς συναίνεσης.

Κατά την αφαίρεση διπλότυπων αξιολογήθηκαν 1500 άρθρα ως προς την καταλληλότητά τους. Έτσι, με βάση αυτό, επιλέξαμε μόνο εργασίες που σχετίζονταν με τις ερωτήσεις που τέθηκαν εξ αρχής. Σε αυτό το στάδιο, αποκλείστηκε ένας σημαντικός αριθμός μελετών. Τελικά καταλήξαμε σε 69 εργασίες που θεωρήθηκε ότι κάλυπταν περισσότερα τα κριτήρια που τέθηκαν ως βάση της έρευνάς μας. Στη συνέχεια, όλες οι αναφορές οργανώθηκαν αρχικά με βάση γενικές πληροφορίες (έτος, τίτλος, συγγραφείς, είδος εργασίας) και δεύτερον με βάση πιο συγκεκριμένες κατηγορίες πληροφοριών (αρχιτεκτονική των DAG-based DLT συστημάτων, μηχανισμοί συναίνεσης σε DAG δίκτυα, προκλήσεις (ασφάλεια, επεκτασιμότητα, ιδιωτικότητα), εφαρμογές των DAG-based DLT-περιπτώσεις χρήσης

Η ανάλυση δεύτερου επιπέδου περιελάμβανε μια εις βάθος ποιοτική ανάλυση περιεχομένου των επιλεγμένων δημοσιεύσεων. Σε αυτό το τελικό στάδιο, χρησιμοποιήθηκε ανάλυση περιεχομένου για την ενδελεχή διερεύνηση και κατηγοριοποίηση της βιβλιογραφίας. Η ανάλυση περιεχομένου πραγματοποιήθηκε διαβάζοντας αυστηρά κάθε επιλεγμένη εργασία, προκειμένου να δημιουργηθεί ένα πιο προσανατολισμένο ερευνητικό πλαίσιο σύμφωνα με τα ερωτήματα που τέθηκαν στην αρχή της εργασίας.

Αφού ολοκληρώθηκε η αναζήτηση βιβλιογραφίας, διαβάσαμε και αναλύσαμε προσεκτικά τα 68 άρθρα για να εντοπίσουμε την αρχιτεκτονική και τους μηχανισμούς συναίνεσης του Shimmer Network και των DAG-based Distributed Ledger Technologies.

Οι μελέτες που πληρούσαν τα προκαθορισμένα κριτήρια χρησιμοποιήθηκαν για τη σύνθεση των αποτελεσμάτων της παρούσας ανασκόπησης.

Η κατηγοριοποίηση των 71 πηγών είναι:

A. Επιστημονικά περιοδικά και συνέδρια με κρίση

[1], [2], [5], [6], [7], [8], [9], [10], [12], [13], [14], [15], [16], [17], [18], [19], [21], [22], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [38], [39], [41], [42], [43], [45], [48], [49], [50], [51], [52], [53], [54], [55], [56], [57], [58], [59], [61], [62], [63], [64], [65]

Σύνολο: 53

B. Προδημοσιεύσεις – Preprints / arXiv

Σύνολο: 6

Γ. Βιβλία, διατριβές, white papers και λοιπές τεχνικές πηγές

[3], [4], [11], [20], [23], [24], [37], [40], [44], [46], [47] [60].

Σύνολο: 12

Πίνακας 3.1. Πίνακας βιβλιογραφικής αναζήτησης

Κωδικός	Query
Q1	("IOTA" OR "Shimmer Network") AND ("DAG")
Q2	("IOTA") AND ("Consensus Mechanism")
Q3	("Shimmer Network") AND ("Security")
Q4	("Shimmer Network") AND ("Scalability")
Q5	("DAG DLT") AND ("Distributed Ledger Technology")

Κεφάλαιο 4ο: Αρχιτεκτονική των DAG-based DLT συστημάτων

4.1 Παραδοσιακή αρχιτεκτονική Blockchain

Τα DLT έχουν γίνει αρκετά δημοφιλή την τελευταία δεκαετία λόγω του ευρέος φάσματος εφαρμογών τους. Η πιο γνωστή αρχιτεκτονική DLT είναι το Blockchain, το οποίο εισήχθη στο κρυπτονόμισμα Bitcoin. Μετά την έλευση του Bitcoin, υπήρξε πληθώρα κρυπτονομισμάτων με παρόμοιες υποκείμενες δομές blockchain, αλλά που διέφεραν ως προς τη συναίνεση, τις εγγυήσεις ασφαλείας, την απόδοση και τις πρόσθετες λειτουργίες. Παρ' όλα αυτά, το κύριο τεχνικό εμπόδιο για την υιοθέτηση του blockchain σε εφαρμογές πραγματικού κόσμου είναι η επεκτασιμότητά του (Raikwar et al. 2025).

Από την έναρξή του, το blockchain έχει θεωρηθεί ως μια χρηματοοικονομική τεχνική, με το Bitcoin να χρησιμεύει ως η πρώτη επιτυχημένη εφαρμογή. Αργότερα, το blockchain έχει ενσωματωθεί με πολλά συστήματα πληροφοριών για την προώθηση της αμετάβλητης φύσης των δεδομένων, της εμπιστοσύνης και της αξιοπιστίας, καθώς γίνεται αντιληπτό ότι το blockchain έχει περισσότερες δυνατότητες από ένα απλό χρηματοοικονομικό εργαλείο. Ωστόσο, τα συμβατικά blockchain έχουν αποδειχθεί αναποτελεσματικά τόσο σε οικονομικές εφαρμογές (π.χ. κρυπτονομίσματα) όσο και σε γενικές εφαρμογές (π.χ. έξυπνα συμβόλαια, ψηφιακά στοιχεία) και ανέκδοτα να χειριστούν αποτελεσματικά ασταθή δίκτυα. Αυτά τα μειονεκτήματα εμποδίζουν μια ευρύτερη χρήση και ανάπτυξη του blockchain. Επιπλέον, έχει εντοπιστεί ότι οι παραδοσιακές δομές blockchain είναι ακατάλληλες για περιβάλλοντα IoT όπου θα δημιουργηθεί μεγάλος όγκος πληροφοριών από τις μαζικές αναπτύξεις συσκευών IoT. Για την αντιμετώπιση αυτού του ζητήματος, έχουν γίνει βελτιστοποιήσεις για διαφορετικά υπόβαθρα υλοποίησης, π.χ., χρησιμοποιώντας blockchain για τη βελτίωση της ασφάλειας των δεδομένων. Παρά τα αξιοσημείωτα επιτεύγματα στη δομή blockchain, οι ερευνητές διαπίστωσαν ότι οι παραδοσιακές δομές που βασίζονται σε αλυσίδες και οι τροποποιήσεις τους δεν μπορούσαν να ικανοποιήσουν τις ολοένα και πιο πολλές και ποικίλες απαιτήσεις των εφαρμογών blockchain (Wu et al. 2022).

Η αρχική έρευνα σχετικά με την τροποποίηση της δομής του blockchain επικεντρώθηκε στην διαισθητική τροποποίηση της δομής των μπλοκ και του κρίκου της αλυσίδας. Για παράδειγμα, ορισμένοι ερευνητές πρόσθεσαν στοιχεία στο μπλοκ ή την αλυσίδα για να επιτύχουν τις λειτουργίες που δεν παρέχει το τυπικό blockchain (όπως το Bitcoin). Αυτές οι τροποποιήσεις βασίζονται άμεσα στη συμβατική δομή μπλοκ. Άλλοι ερευνητές άλλαξαν τη δομή του κρίκου της αλυσίδας, είτε με την προσθήκη ειδικών μπλοκ στην αλυσίδα (Arthurs et al. 2022), είτε με την προσθήκη πολλαπλών προηγούμενων μπλοκ αντί της εφαρμογής μόνο ενός προηγούμενου μπλοκ (Zhang, et al. 2023) είτε με την προσθήκη επιπλέον αλυσίδων (Jalalmaal, et al 2019). Για την υποστήριξη μοναδικών περιβαλλόντων υπηρεσιών, π.χ., IoT και αναζήτηση δεδομένων, προτάθηκε μια σημαντική παραλλαγή του blockchain, η δισδιάστατη αλυσίδα. Στη συνέχεια, προτάθηκαν παρόμοιες δομές, γνωστές ως Προσαρτήσιμες αλυσίδες. Ελαφρώς διαφορετικές από την δισδιάστατη αλυσίδα, οι κάθετες αλυσίδες των Προσαρτήσιμων αλυσίδων κατασκευάζονται από τις συναλλαγές του σώματος του μπλοκ, αντί για την πλήρη αλυσίδα που σχηματίζεται από μπλοκ. Παρά τα αξιοσημείωτα επιτεύγματα στη δομή του blockchain, οι ερευνητές διαπίστωσαν ότι οι παραδοσιακές δομές που βασίζονται σε αλυσίδες και οι τροποποιήσεις τους δεν μπορούσαν να ικανοποιήσουν τις ολοένα και πιο πολλές και ποικίλες απαιτήσεις των εφαρμογών blockchain (Wu et al. 2022).

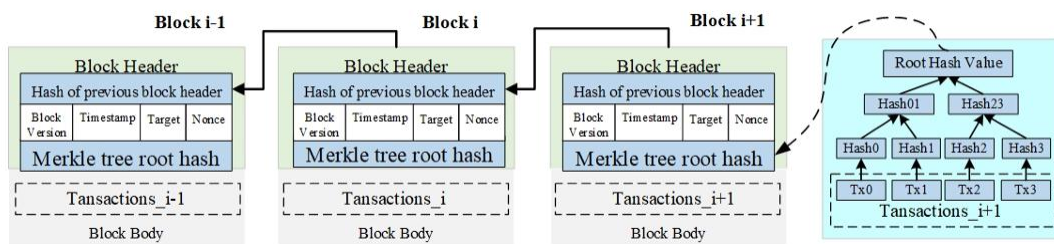
Το Blockchain είναι η πρώτη γενιά τεχνολογίας κατανεμημένου καθολικού. Το πιο αντιπροσωπευτικό σύστημα blockchain είναι το Bitcoin. Η υποκείμενη συνολική δομή προέρχεται από το Bitcoin ως blockchain, το οποίο υποδηλώνει μια αλυσίδα μπλοκ. Το Σχήμα (εικόνα 4.1) δείχνει τη γενική δομή

ενός συστήματος blockchain. Το βασικό στοιχείο στο blockchain είναι το μπλοκ. Κάθε μπλοκ, εκτός από το μπλοκ γένεσης, δείχνει σε ένα προηγούμενο μπλοκ μέσω της συνάρτησης κατακερματισμού. Δηλαδή, κάθε μπλοκ δείχνει στο κατακερματισμό του προηγούμενου μπλοκ, επομένως σχηματίζει μια αμετάβλητη αλυσίδα, με τις ιδιότητες του αλγορίθμου κατακερματισμού. Ένα μπλοκ συνήθως δημιουργείται από το κατακερματισμό, τη χρονική σήμανση, την nonce, το Merkle tree και τις συναλλαγές, για να υποστηρίξει τη συνάρτηση κρυπτονομισμάτων που κατέχει το blockchain. Γενικά, οι εφαρμογές που βασίζονται σε blockchain χρησιμοποιούν μια παρόμοια δομή αλυσίδας μπλοκ με το συμβατικό blockchain (κρυπτονομίσματα). Για να περιγραφεί μια τέτοια δομή με μεγαλύτερη ακρίβεια, παρέχεται η ακόλουθη περιγραφή: Ένα blockchain B αποτελείται από ένα σύνολο μπλοκ $\mathcal{B}$, ένα σύνολο συνδέσμων $\mathcal{E}$, τον κανόνα του συνδέσμου $\mathcal{C}$ και ένα σύνολο διατεταγμένων συναλλαγών $\mathcal{T}$. Κάθε μπλοκ $b \in \mathcal{B}$ συνδέεται ένα προς ένα μέσω των συνδέσμων στο $\mathcal{E}$, και κάθε δύο μπλοκ συνδέονται με έναν κατευθυνόμενο σύνδεσμο που ακολουθεί το $\mathcal{C}$, και συνήθως δείχνει από το νεότερο προς το προηγούμενο μέσω του αλγορίθμου κατακερματισμού, δηλαδή, ο τελευταίος δείχνει στον κατακερματισμό του πρώην. Κάθε μπλοκ b αποτελείται από ένα διατεταγμένο υποσύνολο $\mathcal{C} \subset \mathcal{T}$, οποιοδήποτε

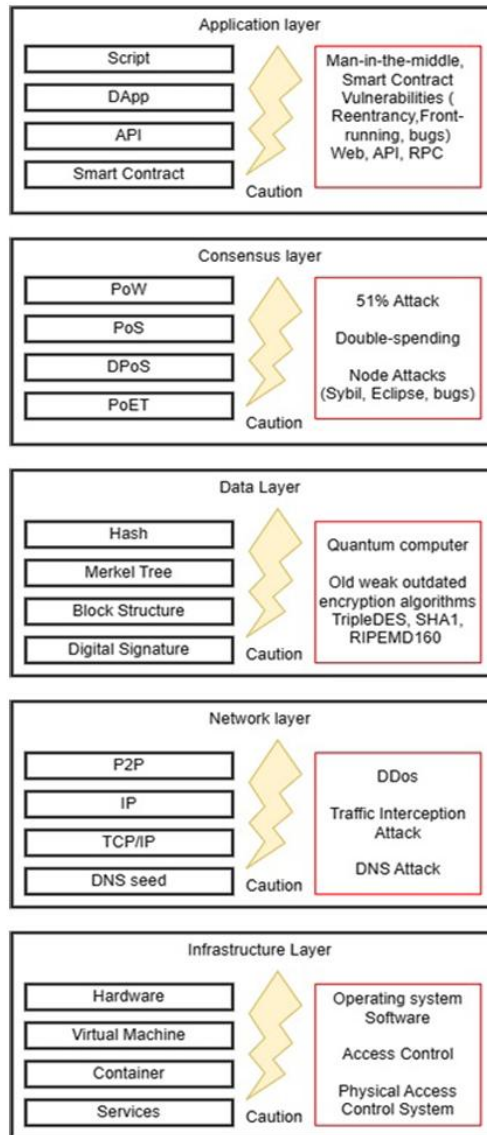
$$(\neq)$$

$\cap = \emptyset$. Κάθε μπλοκ b περιλαμβάνει ένα δέντρο Merkle $\mathcal{M}$, καθώς και ορισμένα γενικά στοιχεία I , όπως χρονική σήμανση και μηδενική τιμή.

Τα περισσότερα συστήματα που βασίζονται σε blockchain χρησιμοποιούν τη δομή που ορίζεται στον προηγούμενο Ορισμό ως την υποκείμενη τοπολογία. Σε αυτήν τη δομή, κάθε μπλοκ αποτελείται από την κεφαλίδα του μπλοκ που περιέχει ένα δέντρο Merkle και το σώμα του μπλοκ που αποθηκεύει τις συναλλαγές. Η γενική κεφαλίδα του μπλοκ θα μπορούσε επίσης να περιλαμβάνει άλλα στοιχεία, όπως χρονική σήμανση, μέγεθος μπλοκ, τιμή nonce, δυσκολία κ.λπ. Να σημειωθεί ότι τα συστήματα που βασίζονται σε blockchain θα μπορούσαν να περιέχουν διαφορετικά στοιχεία στην κεφαλίδα ανάλογα με τον συγκεκριμένο σχεδιασμό του συστήματος. Για παράδειγμα, τα συστήματα που χρησιμοποιούν την Πρακτική Βυζαντινή Ανοχή Σφαλμάτων (PBFT) δεν χρειάζονται τιμή nonce και δυσκολία. Παρ'όλα αυτά, η τοπολογία της αλυσίδας συνήθως παραμένει αμετάβλητη σε διαφορετικά συστήματα που βασίζονται σε blockchain (Wu et al 2022).



Εικόνα 4.1 Η δομή του blockchain. Πηγή: Zhou et al. ((2023))



Εικόνα 4.2 Αρχιτεκτονική του blockchain Πηγή: Baboi (2023)

4.2 Αρχιτεκτονικές DAG-based DLT

Η ιδέα της DLT που βασίζεται σε DAG είναι να σχηματίσει μια κατευθυνόμενη ακυκλική δομή γραφήματος από τα μπλοκ/συναλλαγές, αντί να σχηματίζει μια αλυσίδα με αναφορά σε ένα μόνο μπλοκ. Με αυτόν τον τρόπο, πολλές συναλλαγές επαληθεύονται παράλληλα, και ως εκ τούτου παρέχουν μια πιο επεκτάσιμη αρχιτεκτονική DLT. Ο στόχος αυτών των DLT που βασίζονται σε DAG είναι να επιτύχουν υψηλότερη απόδοση διατηρώντας ή μειώνοντας παράλληλα την πολυπλοκότητα επικοινωνίας ή/και υπολογισμού, την καθυστέρηση και την επιβάρυνση αποθήκευσης (Rochman et al., 2023). Η αρχιτεκτονική του IOTA tangle είναι μια εξελισσόμενη πλατφόρμα DLT, που στοχεύει στην αντιμετώπιση ζητημάτων κόστους συναλλαγών, εξόρυξης και επεκτασιμότητας (στο πλαίσιο της τεχνολογίας Blockchain) (Zhang και Jacobsen, 2018), που σχετίζονται με το IoT. Το Tangle μπορεί να χρησιμοποιηθεί για την κατασκευή εφαρμογών IoT (Alsbouei et al. 2023).

Η αρχιτεκτονική κάθε DLT μπορεί περιληπτικά να παρουσιαστεί ως αποτελούμενη από το ίδιο σύνολο επιπέδων. Κάθε επίπεδο έχει σαφώς καθορισμένη λειτουργικότητα, αν και η υλοποίησή τους ποικίλλει μεταξύ των DLT (Raikwar et al. 2025).

—Το επίπεδο δεδομένων είναι υπεύθυνο για την αποθήκευση συναλλαγών και τη διατήρηση της δομής δεδομένων του καθολικού μητρώου.

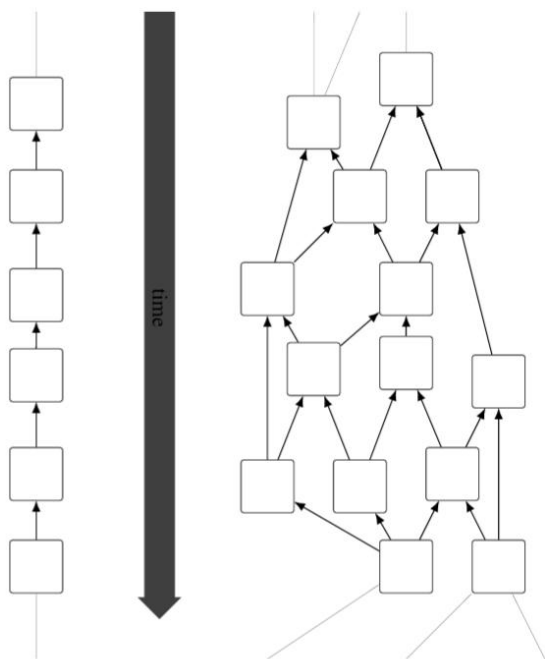
—Το επίπεδο δικτύου είναι υπεύθυνο για την επικοινωνία, π.χ., τη διάδοση δεδομένων κορυφών σε όλους τους κόμβους.

—Το επίπεδο συναίνεσης είναι απαραίτητο για την επικύρωση συναλλαγών και για την επίτευξη συμφωνίας σχετικά με την κατάσταση του συστήματος. Αυτό το επίπεδο δημιουργεί μια κοινή προβολή του ιστορικού συναλλαγών και καθορίζει μια κανονική σειρά συναλλαγών.

—Το επίπεδο έξυπνων συμβάσεων επιτρέπει την ανάπτυξη και εκτέλεση αυτοεκτελούμενων συμφωνιών που κωδικοποιούνται σε λογισμικό. Οι συναλλαγές σε αυτό το επίπεδο αντιπροσωπεύουν μεταβάσεις κατάστασης που ενημερώνουν δεδομένα στην αλυσίδα, εκτελούν λογική συμβολαίων και ενεργοποιούν συμβάντα, βασιζόμενες στη συναίνεση για ντετερμινιστική εκτέλεση και συνέπεια. Το επίπεδο εφαρμογής αντιπροσωπεύει μια αφαίρεση εφαρμογών που βασίζονται στο υποκείμενο DLT. Όταν παρουσιάζεται το πεδίο εφαρμογής της οικοδόμησης γνώσης, αυτό τοποθετείται στο πλαίσιο συγκεκριμένων επιπέδων (Raikwar et al. 2026). Η τεχνολογία κατανεμημένου καθολικού DLT χρησιμοποιώντας ένα πολυεπίπεδο μοντέλο, κατηγοριοποιείται σε αλυσιδωτούς, αλυσιδωτούς και υβριδικούς τύπους, (Bellaj et al. 2022), ενώ υπάρχουν ποικίλες λειτουργικές και δομικές επιλογές εντός των συστημάτων DLT (Kannengießer et al. 2019).

Η τεχνολογία κατανεμημένου καθολικού υπόσχεται να αντιμετωπίσει τα προβλήματα που προέρχονται από τις υπάρχουσες κεντρικές αρχιτεκτονικές Διαδικτύου των Πραγμάτων (IoT). Τα βασικά χαρακτηριστικά του DLT που είναι επωφελή για τις εφαρμογές του IoT περιλαμβάνουν την αποκέντρωση, την αμετάβλητη ικανότητα, την ελεγκτική ικανότητα και την κρυπτογραφική ασφάλεια. Η αποκέντρωση επιτρέπει την ανταλλαγή πληροφοριών σε ολόκληρο το δίκτυο μέσω επικοινωνίας peer-to-peer (P2P), εξαλείφοντας την ανάγκη για επικύρωση ή έλεγχο από ένα εξουσιοδοτημένο και αξιόπιστο κεντρικό τρίτο μέρος. Αυτό μπορεί να μειώσει το κόστος του συστήματος, καθώς δεν απαιτείται πλέον η συντήρηση και η λειτουργία του εν λόγω κεντρικού κύριου διακομιστή. Η αμετάβλητη ικανότητα αποτρέπει την παραποίηση δεδομένων και διευκολύνει την πλήρη παρακολούθηση του ιστορικού όλων των ανταλλαγών δεδομένων. Η ελεγκτική ικανότητα είναι σημαντική για τα δίκτυα IoT, καθώς κάθε συσκευή έχει την επιλογή να αποθηκεύσει ένα πλήρες αντίγραφο του καθολικού, εάν απαιτείται, και τα αρχεία συναλλαγών με χρονική σήμανση διασφαλίζουν ότι όλες οι συναλλαγές και οι ανταλλαγές δεδομένων είναι επαληθεύσιμες (Raikwar et al. 2025)

Κάθε DLT χρησιμοποιεί έναν μοναδικό κρυπτογραφικό αλγόριθμο για να ασφαλίσει το πρωτόκολλό του, το οποίο εξοπλίζει τα δίκτυα IoT με ανθεκτικότητα έναντι επιθέσεων. Μερικοί από τους χρησιμοποιούμενους κρυπτογραφικούς αλγόριθμους, όπως αυτοί που αξιοποιούν σχήματα υπογραφής μίας χρήσης, είναι κβαντικά ασφαλείς, ενώ εκείνοι που χρησιμοποιούν κρυπτογράφηση RSA ή ελλειπτικής καμπύλης, είναι ευάλωτοι σε επιθέσεις από κβαντικούς υπολογιστές (Sealey et al 2022)



Εικόνα 4.2 Blockchain και blockDAG (Πηγή: Raikwar et al. 2025)

4.3 IOTA Tangle

Σήμερα, οι Τεχνολογίες Κατανεμημένου Καθολικού (DLT) αποτελούν μια άλλη σχετική και βιώσιμη επιλογή για την υποστήριξη της ανταλλαγής δεδομένων, αξιοποιώντας παράλληλα σημαντικά χαρακτηριστικά ασφαλείας, όπως η αμετάβλητη και η επαληθευσσιμότητα των δεδομένων. Όταν πρόκειται για συστήματα αισθητήρων που παράγουν δεδομένα με υψηλή απόδοση, το IOTA Tangle στη νέα του έκδοση Chrysalis είναι μια πολύτιμη επιλογή κατά τη γνώμη των Carelli et al. (2022).

Το IOTA Tangle είναι μια τεχνολογία κατανεμημένου καθολικού (DLT), σχεδιασμένη κυρίως για δίκτυα και εφαρμογές του Διαδικτύου των Πραγμάτων (IoT). Το IOTA Tangle χρησιμοποιεί μια δομή άμεσου ακυκλικού γραφήματος (DAG) για το καθολικό, με το πρωτόκολλό του να προσφέρει χαρακτηριστικά ελκυστικά για τον τομέα του IoT, σε σχέση με τις περισσότερες εναλλακτικές λύσεις blockchain, όπως αβλαβείς συναλλαγές, υψηλότερες εφικτές συναλλαγές ανά δευτερόλεπτο (TPS) και χαμηλότερη κατανάλωση ενέργειας.

Το Tangle της IOTA που βασίζεται σε Directed Acyclic Graph (DAG) αντιπροσωπεύει μια θεμελιώδη απόκλιση από τις παραδοσιακές αρχιτεκτονικές blockchain. Σε αντίθεση με τα συστήματα blockchain, όπου οι συναλλαγές ομαδοποιούνται σε μπλοκ και προστίθενται διαδοχικά, το Tangle επεξεργάζεται τις συναλλαγές ασύγχρονα. Κάθε συναλλαγή επικυρώνει δύο προηγούμενες συναλλαγές, δημιουργώντας έναν μηχανισμό παράλληλης επεξεργασίας που εξαλείφει τα σημεία συμφόρησης, που είναι εγγενή στις αρχιτεκτονικές blockchain. Αυτός ο σχεδιασμός επιτρέπει στο IOTA να επιτυγχάνει υψηλή επεκτασιμότητα και αποτελεσματικότητα, καθιστώντας το ιδιαίτερα κατάλληλο για περιβάλλοντα IoT, όπου οι συσκευές δημιουργούν συχνές, μικρής κλίμακας ανταλλαγές δεδομένων (Ramírez-Gordillo et al 2025).

Το Tangle είναι το πρωτόκολλο ή η δομή δεδομένων μια συλλογή από κόμβους και βέλη, που χρησιμοποιείται στο IOTA για την αποθήκευση των συναλλαγών. Όλες οι κορυφές ή οι κόμβοι που

περιέχουν δεδομένα (συναλλαγές) συνδέονται μεταξύ τους μέσω ακμών, που χρησιμοποιούνται για τον έλεγχο της έγκυρης συναλλαγής, ώστε να επιτευχθεί τελικά η έγκριση ή η επιβεβαίωση της συναλλαγής. Το Genesis είναι η πρώτη ή η μοναδική τοποθεσία που δεν έχει καμία προηγούμενη τοποθεσία ή γονείς (Serguei, 2017). Η αρχιτεκτονική Tangle μέσω διαφόρων κόμβων QubicNodes, Full Nodes, Light Node και Masked Authentication Messaging έχει χρησιμοποιηθεί για την επίτευξη κατανεμημένης νοημοσύνης στο IoT. (Alsbouei et al. 2019).

Νέες συναλλαγές μπορούν να προστίθενται συνεχώς στο tangle χρησιμοποιώντας έναν αλγόριθμο επιλογής tip. Υπάρχουν 3 διαθέσιμες μέθοδοι που χρησιμοποιεί γενικά το IOTA, όπως είναι η Ομοιόμορφη Επιλογή Τυχαίων Συμβουλών (URTS), η Μη Βαρυμένη Τυχαία Εργασία (URW) και η Βαρυμένη Τυχαία Εργασία (WRW) (Rochman et al. 2022)

Η αρχική υλοποίηση του IOTA βασιζόταν σε μια λύση κεντρικού συντονιστή bootstrap για συναίνεση, η οποία περιόριζε τον βαθμό αποκέντρωσης και επεκτασιμότητας. Αυτή η ανησυχία, μαζί με άλλους περιορισμούς στην υιοθέτησή του, όπως η έλλειψη έξυπνων συμβολαίων, αντιμετωπίζονται με την κυκλοφορία του IOTA 2.0. Αυτή η ενημέρωση φέρνει μαζί της σημαντικές αλλαγές προκειμένου να αφαιρεθεί ο συντονιστής και να επιτευχθεί μια επεκτάσιμη αποκεντρωμένη λύση (Sealey et al 2022).

Το IOTA έχει προγραμματιστεί να υποβληθεί σε μια αναβάθμιση πρωτοκόλλου δύο μερών, το IOTA 1.5 (Chrysalis), το οποίο είναι το τρέχον δίκτυο, και το IOTA 2.0 (Coordicide), με στόχο την εφαρμογή μιας σειράς σημαντικών τεχνολογικών εξελίξεων DLT για τη βελτίωση της λειτουργικότητας του δικτύου και την επίτευξη μεγαλύτερης αποκέντρωσης. Το IOTA 2.0 εφαρμόζει έναν νέο μηχανισμό συναίνεσης που στοχεύει στη βελτίωση της επεκτασιμότητας, της ασφάλειας και της αποκέντρωσης του IOTA, αφαιρώντας τον κεντρικό κόμβο Coordinator (Alsbouei et al., 2023). Στην εργασία των Sealey et al (2022) παρουσιάζονται τα βασικά χαρακτηριστικά του IOTA 2.0., ενώ παράλληλα συζητιούνται και τα οφέλη τους για το ευρύτερο οικοσύστημα του IoT.

Το IOTA 2.0 έχει ενσωματώσει ανθεκτικούς μηχανισμούς για τον μετριασμό των συνεπειών των επιθέσεων άρνησης υπηρεσίας (DoS). Παρ' όλα αυτά, η συνεχής ανάπτυξη και οι δοκιμές δείχνουν ότι το δίκτυο δεν είναι εντελώς άτρωτο σε τέτοιες απειλές. Το Ίδρυμα IOTA και η κοινότητά του προσπαθούν συνεχώς να ενισχύσουν την ασφάλεια και την επεκτασιμότητα του δικτύου, τους πεπερασμένους πόρους που μειώνονται με την πάροδο του χρόνου και, ως εκ τούτου, εμποδίζουν την παρατεταμένη συσσώρευσή τους. Επιπλέον, προτάθηκε από τους Fartitchou et al. (2024), η ενσωμάτωση ενός ανιχνευτή DoS που βασίζεται σε έξυπνα συμβόλαια, ο οποίος είναι κρίσιμος για την προληπτική αντιμετώπιση πιθανών απειλών, ενισχύοντας έτσι την ασφάλειά του συστήματος. Το σύστημά περιλαμβάνει παρόχους υπηρεσιών Διαδικτύου (ISP), με τον καθένα να επιβλέπει τον δικό του αποκλειστικό ελεγκτή που συνδέεται με ένα σύνολο διακοπών, λειτουργώντας ως κύριοι διαχειριστές και εφεδρικοί ελεγκτές για άλλους τομείς. Οι συνεργατικές προσπάθειες μεταξύ των παρόχων υπηρεσιών Διαδικτύου (ISP) είναι απαραίτητες για την επέκταση της κάλυψης του δικτύου σε διάφορους τομείς των ISP. Είναι επιτακτική ανάγκη να παρακολουθείται αυτή η συνεργασία για να αποτρέπεται η παραβίαση κανονισμών από οποιονδήποτε ISP ή η ανεξάρτητη λειτουργία εντός του δικτύου. Οι συμβάσεις που σχεδιάστηκαν καθιερώνουν ένα πλαίσιο ελέγχου πρόσβασης για τους ελεγκτές, διασφαλίζοντας ασφαλή, ρυθμιζόμενη και καλά οργανωμένη συνεργασία στις λειτουργίες του δικτύου. Αυτό το οικοσύστημα περιλαμβάνει τρεις βασικούς παράγοντες, όπως φαίνεται στην εικόνα 4.4 (Fartitchou et al.2024).

Οι διαφοροποιητικές πτυχές του IOTA 2.0 μπορούν να χωριστούν σε ενότητες προκειμένου να κατανοηθεί ο αντίκτυπός τους στο συνολικό πρωτόκολλο καθώς και στις εφαρμογές του IoT. Ορισμένες από τις βασικές διαφορές μεταξύ του παλαιού IOTA και του IOTA 2.0, φαίνονται στον πίνακα 1. Η εικόνα 2 παρέχει μια ολιστική άποψη της συνολικής δομής και λειτουργίας του πρωτοκόλλου του IOTA 2.0. Το επίπεδο δικτύου χειρίζεται τη λειτουργικότητα του κόμβου Tangle

που λειτουργεί με bytes και επομένως περιλαμβάνει όλες τις ανταλλαγές P2P (μεταξύ κόμβων). Το επίπεδο επικοινωνίας χειρίζεται τα μηνύματα IOTA. Αυτό περιλαμβάνει τις απαιτούμενες εγκρίσεις επιλογής φιλοδοWRήματος, τους μηχανισμούς ελέγχου ρυθμού, καθώς και τον χειρισμό του ίδιου του καθολικού Tangle. Το επίπεδο εφαρμογής ασχολείται με την εκτέλεση ωφέλιμων φορτίων μηνυμάτων. Για παράδειγμα, για μια συναλλαγή αξίας, εκτελεί την απαιτούμενη συναίνεση, τις μεταφορές κεφαλαίων και τη μεταφορά φήμης (mana). Τονίζεται ότι κάθε μία από τις ενότητες που παρουσιάζονται βρίσκεται υπό συνεχή αναθεώρηση και ανάπτυξη από το Ίδρυμα IOTA. (Sealey et al 2022).

Οι συναλλαγές στο Tangle δεν απαιτούν χρεώσεις και οι κόμβοι του δικτύου επικυρώνουν συνεχώς τις συναλλαγές με πλήρη ταχύτητα. Μια συναλλαγή θεωρείται έγκυρη όταν έχει μια αναφορά σε μια ειδική που ονομάζεται ορόσημο. Η Απόδειξη Εργασίας (PoW) δεν προορίζεται να αποτελέσει μέρος της διαδικασίας επικύρωσης, επομένως για να ασφαλίσει το δίκτυο όπως στα blockchains, αλλά μόνο για να αποθαρρύνει τις ανεπιθύμητες συναλλαγές στο Tangle. Ένας κόμβος που είναι πρόθυμος να μεταδώσει μια νέα συναλλαγή μέσω του δικτύου αναμένεται να επικυρώσει δύο προηγούμενες συναλλαγές. Με αποτέλεσμα όσο περισσότερες οι εισερχόμενες συναλλαγές, τόσο πιο γρήγορη είναι η συναίνεση και η επικύρωση συναλλαγής. Κατ' αρχήν, η συνολική απόδοση είναι άπειρη, στην πράξη, η PoW χαμηλής πολυπλοκότητας και η διαδικασία συναίνεσης καθορίζουν το όριο απόδοσης. Οι αρχές λειτουργίας του Tangle, το καθιστούν κλιμακωτό, ανάλογα με τον αριθμό των εισερχόμενων συναλλαγών και επομένως μια επιλογή για την εξυπηρέτηση του κόσμου του IoT και των αισθητήρων. Επιπλέον, το Tangle έχει σχεδιαστεί για να προσφέρει τη δυνατότητα αποθήκευσης δεδομένων με μια συναλλαγή ενός ειδικού μηνύματος που φέρει ένα ωφέλιμο φορτίο τύπου ευρετηρίασης. Μια συναλλαγή με ένα μήνυμα ευρετηρίασης αγκυρώνει τα δεδομένα στο Tangle. Οποιοσδήποτε κόμβος που είναι πρόθυμος να καταναλώσει αυτά τα δεδομένα τα ανακτά στο καθορισμένο ευρετήριο. Ένα πρωτόκολλο που λειτουργεί στο Επίπεδο 2 (L2) (δηλαδή, πάνω από το Επίπεδο 1 του IOTA που είναι υπεύθυνο για την αλληλεπίδραση με το Tangle), χρησιμοποιείται για τη δομή δεδομένων μέσω του Tangle και επιτρέπει (i) τη μετάδοση σύνθετων ροών δεδομένων και (ii) την απλή ανάκτηση δεδομένων. Ένα τέτοιο πρωτόκολλο L2 είναι ένα κρυπτογραφικό πρωτόκολλο που εξασφαλίζει τη μετάδοση δεδομένων από άκρο σε άκρο μέσω του Tangle. Παρέχει τα πρωτόγονα για τη δομή μιας ροής δεδομένων μέσω του Tangle, για την απόδειξη της πηγής δεδομένων και της ιδιοκτησίας των δεδομένων, για την κρυπτογράφηση και αποκρυπτογράφηση δεδομένων και για την εύκολη ανάκτηση και κατανάλωση της ροής δεδομένων κατά την επαλήθευσή της. Το ίδιο το Tangle παρέχει αμεταβλητότητα και ακεραιότητα δεδομένων (Carelli et al. 2022).

Ο συνδυασμός ενός κρυπτογραφικού πρωτοκόλλου L2 και του Tangle είναι ένα εναλλακτικό μέσο ασφαλούς μεταφοράς στο TLS, επιτρέποντας την ασφαλή μεταφορά δεδομένων από πολλαπλά σημεία σε πολλαπλά σημεία. Αυτός ο συνδυασμός παρέχει ένα επίπεδο εμπιστοσύνης για οποιοδήποτε καταναμεμημένο σύστημα αισθητήρων για την ασφαλή ανταλλαγή δεδομένων σε (σχεδόν) πραγματικό χρόνο. Όχι μόνο, τα δεδομένα είναι μόνιμα αγκυρωμένα στο Tangle, επομένως μπορούν να επαληθευτούν και να καταναλωθούν ανά πάσα στιγμή, ακόμη και εκ των υστέρων. Για λόγους πληρότητας, η ποιότητα των δεδομένων και η φήμη της πηγής είναι άλλα δύο κύρια σημεία που απαιτούν ιδιαίτερη προσοχή. Αξίζει να σημειωθεί ότι το Tangle είναι μια πιθανή τυποποιημένη διεπαφή για την ανταλλαγή δεδομένων. Ετερογενή και ανεξάρτητα συστήματα, καθένα από τα οποία έχει σχεδιαστεί για να εξυπηρετεί έναν συγκεκριμένο σκοπό, μπορούν ούτως ή άλλως να αλληλεπιδρούν μεταξύ τους χωρίς την ανάγκη επανασχεδιασμού και ανάπτυξης νέων προσαρμοσμένων διεπαφών ανταλλαγής δεδομένων. Οποιαδήποτε πηγή δεδομένων πρέπει μόνο να παραχωρήσει πρόσβαση στη ροή δεδομένων της στο άλλο σύστημα (Carelli et al. 2022).

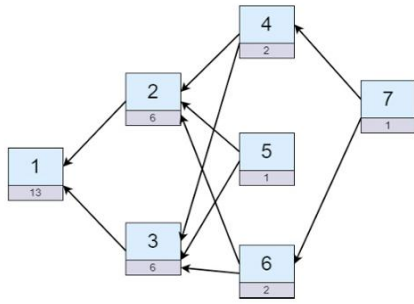
Το Ίδρυμα IOTA ανέπτυξε δύο πρωτόκολλα L2 για τη δομή και την πλοήγηση δεδομένων μέσω του Tangle. Αυτά τα πρωτόκολλα παρουσιάζουν διαφορετικά κρυπτογραφικά χαρακτηριστικά, αλλά παρουσιάζουν επίσης ένα κοινό μειονέκτημα, δηλαδή, έχουν σχεδιαστεί για να λειτουργούν σε ένα σύστημα πλήρους λειτουργικότητας αλλά όχι σε συσκευές με περιορισμούς. Το πρώτο είναι το Masked Authenticated Messaging (MAM) και το δεύτερο είναι το STREAM.

Το MAM λειτουργεί με μια παλαιότερη έκδοση του IOTA Tangle, χρησιμοποιεί τριαδική κωδικοποίηση και κβαντική κρυπτογραφία και έχει αναπτυχθεί σε γλώσσα Javascript.

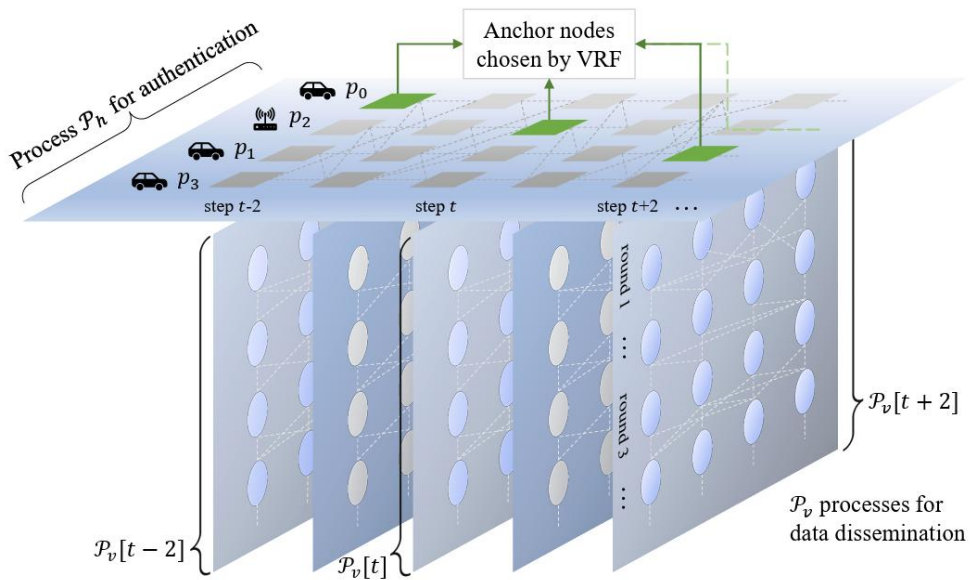
Το παλαιότερο IOTA Tangle εισήγαγε, για πρώτη φορά, την έννοια των συναλλαγών μηδενικής αξίας για την εγγραφή δεδομένων στο Tangle. Το πρωτόκολλο IOTA L1 είναι υπεύθυνο για τη συναλλαγή των δεδομένων, αλλά η συναλλαγή δεν προστατεύεται ή δεν ελέγχεται για τον σκοπό της επαλήθευσης της αυθεντικότητας των δεδομένων. Το MAM είναι το πρωτόκολλο L2 που παρέχει τον τρόπο σε μια συσκευή να προστατεύει και να δομεί ένα δίκτυο δεδομένων μέσω του Tangle και σε οποιεσδήποτε άλλες συσκευές να αποκρυπτογραφούν τη ροή δεδομένων και να επαληθεύουν την αυθεντικότητά της. Το MAM εισήγαγε την έννοια του καναλιού δεδομένων Carelli et al. 2022).

Το πρωτόκολλο MAM έχει καταργηθεί και αντικατασταθεί από το STREAMS. Το STREAM αντικαθιστά το MAM προσθέτοντας νέα ενδιαφέροντα κρυπτογραφικά χαρακτηριστικά και λειτουργεί με τη νέα έκδοση Chrysalis του IOTA Tangle. Το STREAMS έχει αναπτυχθεί σε γλώσσα RUST. Είναι ένα οργανωτικό εργαλείο για τη δομή και την πλοήγηση ασφαλών δεδομένων μέσω του Tangle. Το STREAMS επιτρέπει σε οποιαδήποτε συσκευή να οργανώνει μηνύματα (δηλαδή, δεδομένα) σε μια ομοιόμορφη και διαλειτουργική δομή που υποστηρίζεται από το Tangle, το οποίο εγγυάται την ακεραιότητα και την αμετάβλητη δομή δεδομένων. Επιπλέον, με τις νέες τεχνικές σύνδεσης, κάθε μήνυμα συνδέεται με ένα άλλο, επιτρέποντας τον τρόπο δημιουργίας σύνθετων δομών δεδομένων πιο εύελικτων από την γραμμική αλυσίδα όπως στο MAM. Τόσο το MAM όσο και το STREAMS παρέχουν αποτελεσματικές λύσεις για τη δομή ασφαλών δεδομένων μέσω του Tangle. Το κύριο πρόβλημα αυτών των πρωτοκόλλων είναι ότι δεν διατηρούν την υπόσχεση του οικοσυστήματος IOTA να υποστηρίξει το IoT και τον κόσμο των αισθητήρων. Οι γλώσσες προγραμματισμού που χρησιμοποιούνται για την ανάπτυξη αυτών των πρωτοκόλλων δεν είναι κατάλληλες για συσκευές IoT με περιορισμούς, οι οποίες αντιπροσωπεύουν την πλειονότητα των συσκευών που αναπτύσσονται σε εφαρμογές αισθητήρων πραγματικού κόσμου. Επιπλέον δεν έχουν σχεδιαστεί λαμβάνοντας υπόψη τους τυπικούς περιορισμούς των συσκευών περιορισμού IoT, όπως η υπολογιστική χωρητικότητα η διαθεσιμότητα μνήμης και οι απαιτήσεις για χαμηλή κατανάλωση ενέργειας (Carelli et al 2022).

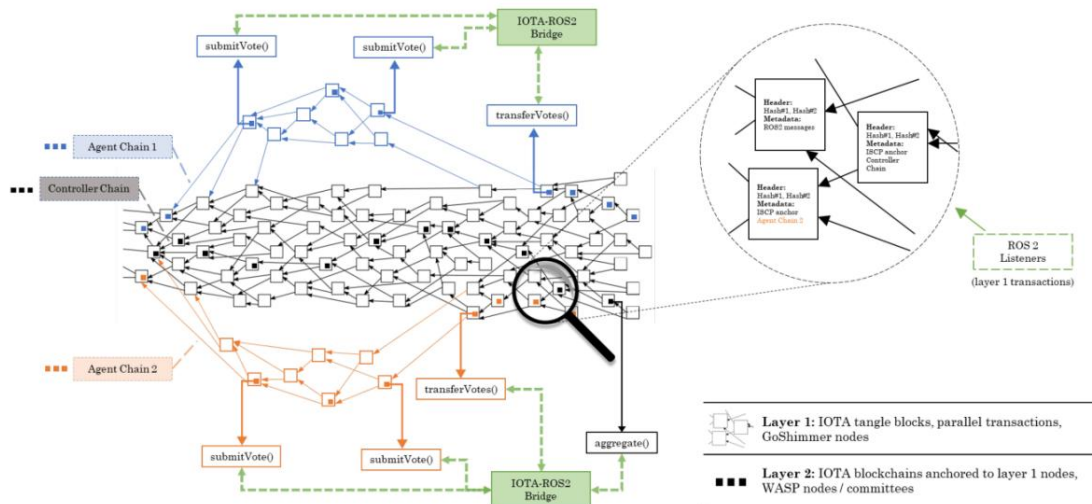
Το πρωτόκολλο L2Sec ορίζει τις αλληλεπιδράσεις μεταξύ ενός κόμβου IoT και του IOTA Tangle. Η πειραματική πλατφόρμα δοκιμών χρησιμοποιεί μία μόνο περιορισμένη συσκευή IoT ως Συγγραφέα και Συνδρομητή. Τα πειράματα δεν λαμβάνουν υπόψη τις αλληλεπιδράσεις μεταξύ διαφορετικών συσκευών, επειδή θα περιλάμβαναν την αξιολόγηση των επιδόσεων του Tangle, κάτι που είναι εκτός του πεδίου εφαρμογής της παρούσας εργασίας. Το πρωτόκολλο L2Sec έχει υλοποιηθεί ως βιβλιοθήκη C πάνω σε ένα firmware bare-metal μαζί με τη βιβλιοθήκη IOTA-C που έχει μεταφερθεί και προσαρμόστηκε για να λειτουργεί σε μικροελεγκτές της οικογένειας STM32. Οι κρυπτογραφικές λειτουργίες αξιοποιούν τη βιβλιοθήκη libsodium. Το L2Sec διατίθεται δωρεάν ως αποθετήριο ανοιχτού κώδικα στο GitHub (Carelli et al 2022).



Εικόνα 4.3 Παράδειγμα ενός IOTA Tangle Πηγή : Rochman et al. (2023).



Εικόνα 4.4 Δισδιάστατη Δομή που βασίζεται σε DAG Πηγή : Wu et al. (2023)



Εικόνα 4.5 Απεικόνιση της ενσωμάτωσης του ROS2 με το πλέγμα IOTA (επίπεδο 1) και τα έξυπνα συμβόλαια IOTA (επίπεδο 2). Το κύριο διαμέρισμα δικτύου, που απεικονίζεται με μαύρο χρώμα, περιλαμβάνει την βασική αλυσίδα CONTROLLER SWARM καθώς και άλλους κόμβους με παγκόσμια συνδεσιμότητα. Με πορτοκαλί και μπλε χρώμα απεικονίζονται δύο παραδείγματα συναλλαγών (αλυσίδες επιπέδου 1 και επιπέδου 2). Πηγή : (Keramat, et al., 2022).

4.4 Αρχιτεκτονική κόμβων και διάδοση συναλλαγών

Το μοντέλο Αδιάθετης Εξόδου Συναλλαγών (UTXO) χρησιμοποιείται συνήθως στον τομέα της Τεχνολογίας Κατανεμημένου Καθολικού (DLT) για τη μεταφορά αξίας μεταξύ των συμμετεχόντων. Το μοντέλο Αδιάθετης Εξόδου Συναλλαγών (UTXO) είναι ένας σχεδιασμός κοινός σε πολλά κρυπτονομίσματα, συμπεριλαμβανομένων των Bitcoin και πολλών παραγώγων του, Cardano και IOTA. Σε ένα μοντέλο UTXO, οι συναλλαγές είναι μεταφορές αξίας από προηγούμενες εξόδους συναλλαγών σε νέες μη δαπανημένες εξόδους με επαγωγικό τρόπο. Οι νέες μη δαπανημένες εξόδους συναλλαγών ονομάζονται UTXO και χρησιμοποιούνται ως εισόδοι για νέες συναλλαγές. (Raikwar et al. 2025). Δηλαδή στο μοντέλο UTXO, οι συναλλαγές ορίζουν τις εξόδους προηγούμενων συναλλαγών ως εισόδους και δημιουργούν νέες εξόδους δαπανώντας τις εισόδους. Έτσι, μια συναλλαγή αποτελείται από μια λίστα εισόδων και μια λίστα εξόδων. Οι εξόδοι σχετίζονται με τις διευθύνσεις των χρηστών μέσω ορισμένων συνθηκών ξεκλειδώματος. Γενικά, ένας λογαριασμός «κατέχει» ένα ιδιωτικό κλειδί και διευθύνσεις που επιτρέπουν την δαπάνη και τη λήψη UTXO. Οι λογαριασμοί στη συνέχεια παρακολουθούν το υπόλοιπό τους διατηρώντας μια λίστα με τις ληφθείσες εξόδους που δεν δαπανήθηκαν. Αυτό το μοντέλο διαφέρει από το άλλο που βασίζεται σε λογαριασμούς και χρησιμοποιείται στα περισσότερα κρυπτονομίσματα που βασίζονται σε έξυπνα συμβόλαια, (πχ. το Ethereum). Το τελευταίο αντιπροσωπεύει τα περιουσιακά στοιχεία ως υπόλοιπα λογαριασμών και οι συναλλαγές περιγράφουν πώς αλλάζουν αυτά τα υπόλοιπα. Μια εννοιολογική διαφορά είναι ότι το μοντέλο που βασίζεται σε λογαριασμούς ενημερώνει τα υπόλοιπα των χρηστών συνολικά, ενώ το μοντέλο UTXO καταγράφει μόνο τις εισπράξεις συναλλαγών. Αυτή η κατασκευή επιτρέπει την παράλληλη επεξεργασία των συναλλαγών, οδηγώντας σε οφέλη απόδοσης και πιθανά

πλεονεκτήματα κλιμάκωσης. Μια άλλη σημαντική διαφορά είναι ότι τα μοντέλα που βασίζονται σε λογαριασμούς χρειάζονται μια συνολική ταξινόμηση για την επίλυση συγκρούσεων, ενώ στο μοντέλο UTXO, αυτή η ταξινόμηση δεν είναι απαραίτητη. Ωστόσο, στην κλιμάκωση παρουσία συγκρουόμενων συναλλαγών υπάρχει μια επίδραση, που δρα περιοριστικά διότι σε αυτήν την περίπτωση, οι συγκρούσεις είναι συναλλαγές που ξόδεψαν την ίδια έξοδο. Καθώς το UTXO Ledger είναι μια δομή μόνο για προσάρτηση, οι συγκρούσεις πρέπει να διευθετηθούν πριν γίνουν αλλαγές. Αυτό γίνεται επί του παρόντος με τη βοήθεια πρωτοκόλλων συναίνεσης που βασίζονται σε έναν (μοναδικό) ηγέτη ή άλλους μηχανισμούς για τη δημιουργία μιας συνολικής ταξινόμησης των συναλλαγών Ένα από τα πλεονεκτήματά του μοντέλου Αδιάθετης Εξόδου Συναλλαγών (UTXO) είναι ότι επιτρέπει την παράλληλη επεξεργασία συναλλαγών, καθώς ανεξάρτητες συναλλαγές μπορούν να προστεθούν με οποιαδήποτε σειρά. Αυτή η ιδιότητα της αναλλοίωτης σειράς και της παραλληλοποίησης πιθανόν να ευνοεί την επεκτασιμότητα. Ωστόσο, δεδομένου ότι το Καθολικό UTXO είναι μια δομή δεδομένων μόνο για προσάρτηση, αυτό το πλεονέκτημα αντισταθμίζεται από την παρουσία αντικρουόμενων συναλλαγών.

Για να επιτρέπεται η παράλληλη επεξεργασία συναλλαγών, το πρώτο βήμα είναι η μετάβαση από την παραδοσιακή δομή blockchain του καθολικού σε μια πιο γενική δομή που βασίζεται σε DAG. Υπάρχουν αρκετές τέτοιες προσεγγίσεις, παρακάμπτοντας τη γραμμική δομή αλυσίδας. Οι περισσότερες από αυτές έχουν κοινό ότι τα μπλοκ μπορούν να αναφέρονται όχι μόνο σε ένα προηγούμενο μπλοκ αλλά και σε περισσότερα από ένα, αλλάζοντας την υποκειμένη δομή δεδομένων από μια αλυσίδα σε ένα κατευθυνόμενο ακυκλικό γράφημα (DAG). Αυτή η φυσική ιδέα της χρήσης DAG έχει γίνει αρκετά δημοφιλής την τελευταία δεκαετία και οδήγησε σε υψηλότερη απόδοση και σε ορισμένες περιπτώσεις σε παρόμοια καθυστέρηση επιβεβαίωσης. Ωστόσο, η παράλληλη γραφή είναι μόνο μια απαραίτητη απαίτηση για την αποτελεσματική παράλληλη επεξεργασία συναλλαγών, αλλά δεν αντιμετωπίζει ακόμη το ζήτημα της επίλυσης συγκρούσεων και της τελικής εκτέλεσης των συναλλαγών (Müller et al., 2023).

4.5 Stardust protocol

Η έκδοση Stardust αποτελεί σημαντική εξέλιξη της αρχιτεκτονικής του Shimmer/IOTA οικοσυστήματος, καθώς εισάγει βελτιωμένους μηχανισμούς διαχείρισης assets και αποδοτικότερη λειτουργία του Tangle. Σύμφωνα με πρόσφατες εμπειρικές μελέτες, το Stardust παρουσιάζει ταχύτερη επιβεβαίωση συναλλαγών και βελτιωμένη αξιοποίηση της DAG δομής σε σχέση με προηγούμενες εκδόσεις. Σύμφωνα με τους Nzakuna et al. (2024) η επιβεβαίωση νέων μπλοκ είναι δύο φορές ταχύτερη στο στάδιο Stardust και το Tangle χρησιμοποιείται επί του παρόντος πολύ κάτω από την ικανότητά του να μεταφέρει και να ασφαλίζει δεδομένα από συσκευές IoT.

94.6 Shimmer Network architecture

Καθώς το IOTA έχει ξεφύγει από το πεδίο εφαρμογής ενός βελτιστοποιημένου DLT για εφαρμογές IoT, το Shimmer συνεχίζει ως ένα DLT βασισμένο σε DAG χωρίς προβλήματα και με την υποστήριξη της κοινότητας. Πριν από την αλλαγή αυτή, αναπτύχθηκαν διαφορετικά πλαίσια βελτιστοποίησης από την ερευνητική κοινότητα, όπως ένα στοχαστικό γενετικό μοντέλο για την παραγωγή συνθετικών δεδομένων Tangle για την εξερεύνηση των επιπτώσεων των ρυθμών άφιξης, οι εξελίξεις στην επιλογή συμβουλών με στόχο τις ταχύτερες επιβεβαιώσεις, καθώς και εφαρμογές ειδικές για συγκεκριμένους τομείς για την ομαλή διανομή δεδομένων (Voulgaridis et al. 2025)

Το Shimmer DLT είναι ένα νέο, άψογο L1 και κλιμακωτό DLT, βασισμένο στην αρχιτεκτονική DAG του δικτύου IOTA που ονομάζεται Tangle, ενώ είναι γνωστό για τη βελτιστοποιημένη δομή του για την υποστήριξη εφαρμογών IoT. Αρχικά, το Shimmer DLT λειτουργούσε ως το δίκτυο σταδιοποίησης για το IOTA Tangle, επιτρέποντας στους προγραμματιστές και τους τελικούς χρήστες να ερευνούν, να αναπτύσσουν και να δοκιμάζουν καινοτόμους μηχανισμούς πριν από την επίσημη ανάπτυξη στο IOTA Tangle. Όπως και το IOTA Tangle, το δίκτυο υποστηρίζεται μέσω κόμβων Hornet, οι οποίοι είναι εξαιρετικά ελαφρείς και μπορούν να εγκατασταθούν από τους τελικούς χρήστες μέσω του ειδικού λογισμικού τους. Οι αρχιτεκτονικές που βασίζονται σε DAG στα DLT ορίζονται από την ικανότητά τους να επιτρέπουν τη δημιουργία και την επιβεβαίωση πολλαπλών μπλοκ συναλλαγών παράλληλα, ξεπερνώντας τα παραδοσιακά blockchains που βασίζονται σε αλυσίδες, όσον αφορά την απόδοση. Συγκεκριμένα, κάθε νέα συναλλαγή που υποβάλλεται και επιβεβαιώνεται εντός της δομής Tangle του Shimmer επαληθεύει δύο προηγούμενες συναλλαγές (Fan et al. 2021). Γενικά, ένας χρήστης είναι σε θέση να υποβάλει μεμονωμένες συναλλαγές, με μέγιστο επιτρεπόμενο μέγεθος έως 32KB (32768 Bytes) (Lin et al. 2024), μέσω της χρήσης του IOTA Software Development Kit (IOTA SDK), με την απαίτηση να διασπαστεί το μήνυμα σε μικρότερα τμήματα εάν το συνολικό του μέγεθος υπερβαίνει το επιτρεπόμενο όριο. Μόλις το μήνυμα προετοιμαστεί στο αποκλειστικό του μπλοκ, δημοσιεύεται στο Shimmer μέσω ενός γνωστού κόμβου Hornet, με τον κόμβο να διαβιβάζει τις σχετικές πληροφορίες στους ομοτίμους του για επιβεβαίωση και εδραίωσή τους.

Το L2Sec είναι ένα κρυπτογραφικό πρωτόκολλο κατάλληλο για συσκευές περιορισμού IoT που βασίζονται σε μικροελεγκτές που έχουν αναπτυχθεί εξ αρχής σε γλώσσα C. Το L2Sec παρέχει όλες τις δυνατότητες μιας συσκευής περιορισμού IoT για να δομήσει μια ροή δεδομένων μέσω του Tangle και να επιτρέψει την ασφαλή ανταλλαγή δεδομένων. Το L2Sec είναι ένα κρυπτογραφικό πρωτόκολλο για τη δομή, την ασφάλεια και την πλοήγηση δεδομένων μέσω του Tangle. Επιπλέον, το L2Sec έχει βελτιωθεί για να αξιοποιήσει ένα Hardware Secure Element για να δημιουργήσει μια ρίζα εμπιστοσύνης υλικού στη συσκευή IoT και να βελτιώσει περαιτέρω την ασφάλεια της συνολικής λύσης με μια προσέγγιση secure-by-design. Το L2Sec έχει σχεδιαστεί, αναπτυχθεί και δοκιμαστεί σε έναν κόμβο IoT του kit STM32L4+ Discovery με το ασφαλές στοιχείο STSAFE A110 (Carelli et al. 2022)

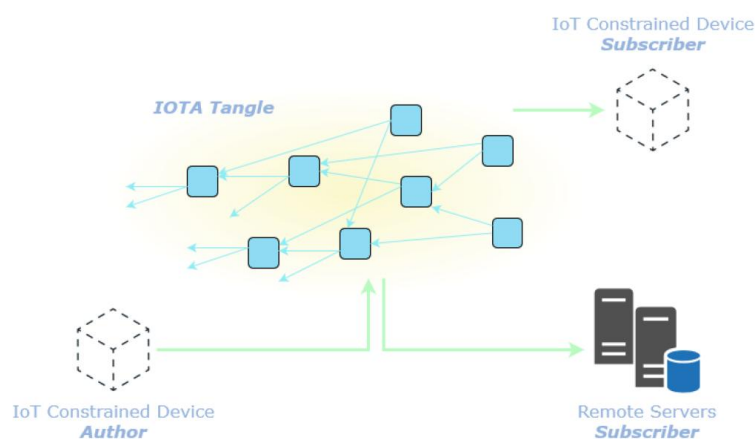
4.7 ShimmerEVM και L1/L2 integration

Το Shimmer είναι το καθορισμένο δίκτυο για το Shimmer EVM, μια λύση Layer 2 που επιτρέπει τον προγραμματισμό έξυπνων συμβολαίων πάνω από το θεμελιώδες επίπεδο (Cech 2020). Το ShimmerEVM διευκολύνει την εκτέλεση έξυπνων συμβολαίων, προσφέροντας ένα αποκεντρωμένο, διαφανές και ασφαλές περιβάλλον χωρίς να βασίζεται στην παραδοσιακή τεχνολογία blockchain. Το επίκεντρο αυτού του συστήματος είναι η εφαρμογή έξυπνων συμβολαίων με επίκεντρο την ασφάλεια. (Maliki et al. 2024)

Το ShimmerEVM είναι ένα δίκτυο δοκιμών στο οικοσύστημα Shimmer, το οποίο έχει σχεδιαστεί ειδικά για να μιμείται το περιβάλλον εικονικής μηχανής Ethereum (EVM) στο Tangle 2.0 του IOTA. Αυτό το δίκτυο επιτρέπει στους προγραμματιστές να αναπτύσσουν και να δοκιμάζουν έξυπνα συμβόλαια σε ένα προσομοιωμένο περιβάλλον Ethereum, αλλά με τα πρόσθετα οφέλη των μοναδικών χαρακτηριστικών του IOTA. Σε αντίθεση με τα παραδοσιακά δίκτυα BC, το ShimmerEVM αξιοποιεί το IOTA Tangle, μια δομή DAG που επιτρέπει την παράλληλη επεξεργασία συναλλαγών, οδηγώντας σε υψηλότερη επεκτασιμότητα, χαμηλότερη κατανάλωση ενέργειας και απρόσκοπτες συναλλαγές. Οι Fartitchou et al. (2024) επέλεξαν το ShimmerEVM για να αξιοποιήσουν αυτά τα πλεονεκτήματα, που

τους επέτρεψαν να αναπτύξουν και να δοκιμάσουν τα έξυπνα συμβόλαια IOTA 2.0 σε ένα ασφαλές, αποτελεσματικό και επεκτάσιμο περιβάλλον πριν τα μεταφέρουμε στο κύριο δίκτυο IOTA (Εικόνα 4 (Fartitchou et al. (2024)).

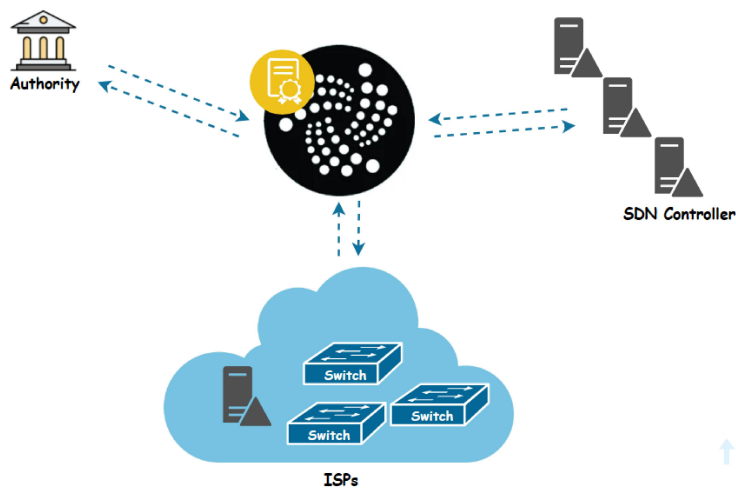
Η έκδοση blockchain IOTA συμβατή με Ethereum και Ethereum Virtual Machine (EVM) που ονομάζεται IOTA-EVM χρησιμοποιείται για την εφαρμογή ενός ισχυρού συστήματος διαχείρισης SLA. Αυτές οι πλατφόρμες blockchain επιτρέπουν τη δημιουργία, την παρακολούθηση και την επιβολή SLA με τρόπο που δεν εμπιστεύεται την εμπιστοσύνη, διασφαλίζοντας ότι οι δεσμεύσεις παροχής υπηρεσιών τηρούνται και ότι τα SLA επιβάλλονται με διαφάνεια και αυτόματα. Οι Muntaha et al. (2024) πρότειναν ένα υβριδικό πλαίσιο βασισμένο σε blockchain για την κοινή χρήση πόρων πολλαπλών χειριστών και τη διαχείριση SLA σε δίκτυα 5G Standalone (5GSA). Στην προτεινόμενη αρχιτεκτονική συστήματος, υιοθέτησαν την αυτόνομη αρχιτεκτονική (SA) 5G. Διαμόρφωσαν μια υβριδική υλοποίηση blockchain δύο επιπέδων για την προτεινόμενη αρχιτεκτονική συστήματος, αξιοποιώντας το Hyperledger Fabric (HLF). Το πλαίσιο ενσωμάτωσε ένα παιχνίδι Stackelberg δύο επιπέδων Multi-Leader Single-Follower (MLSF) για τη μοντελοποίηση τιμολόγησης και στρατηγικών αγοράς. Τα αποτελέσματα κατέδειξαν την αποτελεσματικότητα του πλαισίου στην ενίσχυση της κατανομής πόρων και της επιβολής SLA σε δίκτυα 5G, επισημαίνοντας τις δυνατότητες διαφορετικών πλατφορμών blockchain στη διαχείριση σύνθετων λειτουργιών δικτύου.



Εικόνα 4.6 Αρχιτεκτονική συστήματος υψηλού επιπέδου. Οι συσκευές με περιορισμούς στο IoT λειτουργούν ως Συγγραφείς, παράγοντας δεδομένα και μεταδίδοντάς τα στο Tangle. Οι Συνδρομητές είναι συσκευές με περιορισμούς ή χωρίς περιορισμούς που έχουν πρόσβαση στο Tangle για να ανακτήσουν τα δεδομένα Πηγή: Carelli et al. (2022)

Πίνακας 4.1 Βασικές διαφορές μεταξύ του παλαιού IOTA και του IOTA 2.0 Πηγή: Sealey et al (2022).

Χαρακτηριστικά	IOTA 2.0	Παλαιό IOTA
Υποστηρίζονται	έξυπνες συμβάσεις	Δεν υποστηρίζονται
Υποστήριξη ψηφιακών περιουσιακών στοιχείων	Ναι	Όχι
Μέγεθος συναλλαγής	100 bytes	1700 bytes
Αποκέντρωση	Πλήρως αποκεντρωμένη	Συντονιστής ως σημείο συγκέντρωσης
Προστασία Sybil	Σύστημα φήμης Mana	Κανένα
Πρόληψη ανεπιθύμητης αλληλογραφίας	Ελαφρύ Προσαρμοστικό PoW	PoW
Τύποι διευθύνσεων	Επαναχρησιμοποιήσιμο	Μίας Χρήσης
Μηχανισμός συναίνεσης	FPC δυαδικό πρωτόκολλο ψηφοφορίας	Βαθμισμένη επιλογή συμβουλών MCMC με συντονιστή
Επεκτασιμότητα	Πολύ επεκτάσιμο (αυξημένο TPS με αυξημένο μέγεθος δικτύου)	Περιορισμένη (συντονιστής και ορόσημα περιορισμός επεκτασιμότητας)
Οριστικότητα έγκρισης	Με βάση τη συναινετική έγκριση mana βάρος – όχι ορφανά	Με βάση το μέγεθος βάρους MCMC - ορφανά πιθανά



Εικόνα 4.7 Σύστημα που βασίζεται σε IOTA για SDN. Πηγή: Fartitchou et al (2024)

4.8 Συγκριτική αποτίμηση Blockchain–DAG–Shimmer

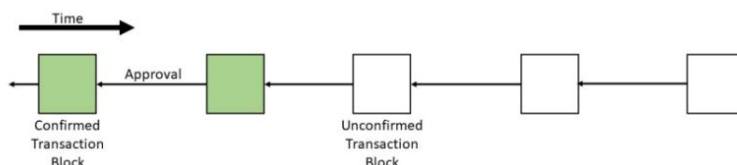
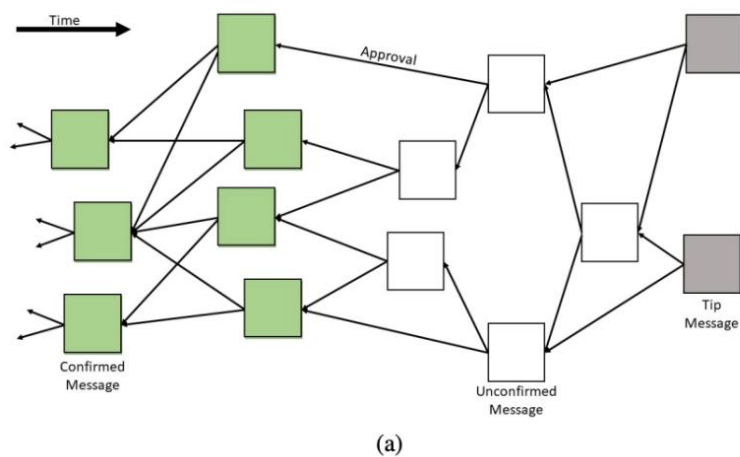
Σε σύγκριση με τα κατανεμημένα καθολικά που βασίζονται σε αλυσίδα, τα καθολικά που βασίζονται σε DAG είναι σχετικά νέες δομές. Μέχρι σήμερα, δεν υπάρχουν κυρίαρχες εφαρμογές επομένως δεν υπάρχει «τυποποιημένη» δομή DAG.

Πίνακας 4.2 Συγκριτική ανάλυση τεχνολογιών Blockchain και DAG Πηγή:

Χαρακτηριστικά	Blockchain	DAG
Αρχιτεκτονική	Αρχιτεκτονική: Ακολουθιακά μπλοκ που αποθηκεύουν πολλαπλές συναλλαγές.	Δομή βασισμένη σε γράφημα με διασυνδεδεμένες συναλλαγές
Μέθοδος επικύρωσης	Χρησιμοποιεί PoW ή PoS για επιβεβαίωση μπλοκ.	Οι συναλλαγές επικυρώνουν η μία την άλλη, καταργώντας την ανάγκη για παραδοσιακή συναίνεση.
Απόδοση	Πιο αργή λόγω περιορισμών εξόρυξης μπλοκ.	Υψηλότερη λόγω παράλληλης επεξεργασίας συναλλαγών.
Επεκτασιμότητα	Περιορίζεται από την αύξηση του φορτίου συναλλαγών.	Εκλιμακώνεται αποτελεσματικά, βελτιώνεται με περισσότερες συναλλαγές.
Αποκέντρωση	Υψηλή αποκέντρωση μέσω συναίνεσης κόμβων.	Η αποκέντρωση μπορεί να ποικίλλει, πιθανώς να μειωθεί εάν η συμμετοχή δικτύου είναι περιορισμένη.
Κόστος Συναλλαγής	Υψηλότερες χρεώσεις λόγω εξόδων εξόρυξης.	Ελάχιστες έως καθόλου χρεώσεις, καθώς δεν απαιτείται εξόρυξη
Κατανάλωση Ενέργειας	Υψηλή, ειδικά σε συστήματα PoW.	Χαμηλότερη, καθώς απουσιάζει η εξόρυξη που καταναλώνει ενέργεια.
Εφαρμογές	Χρησιμοποιείται σε κρυπτονομίσματα, έξυπνα συμβόλαια και αλυσίδες εφοδιασμού.	Κατάλληλο για γρήγορες συναλλαγές, IoT, μικροπληρωμές και δεδομένα σε πραγματικό χρόνο

Πίνακας 4.3 Σύγκριση Blockchain και DAG-based DLT

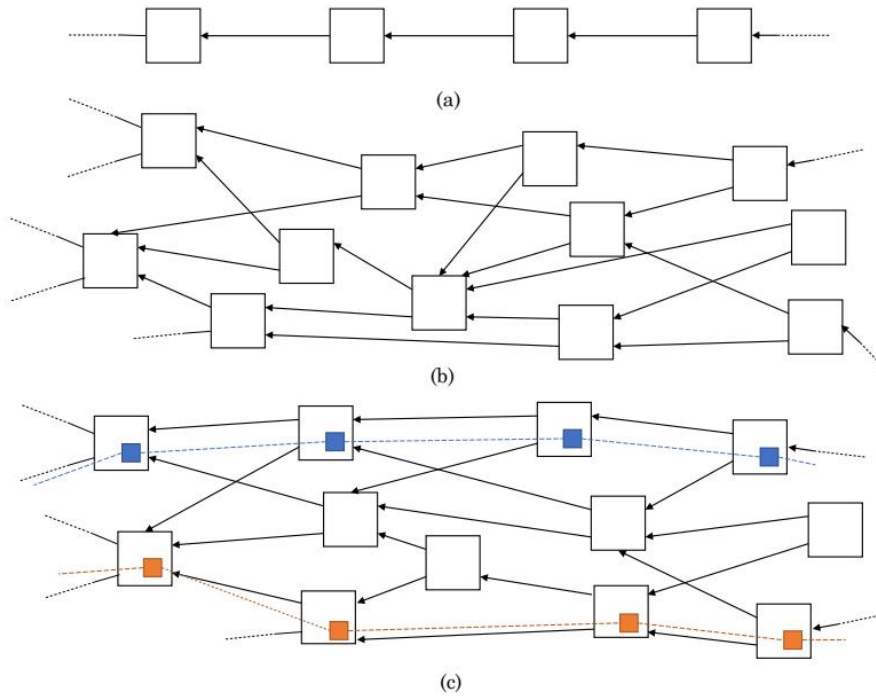
Χαρακτηριστικό	Blockchain	DAG-based DLT
Δομή	Αλυσίδα blocks	Κατευθυνόμενο Ακυκλικό Γράφημα
Επεξεργασία	Διαδοχική	Παράλληλη
Επεκτασιμότητα	Περιορισμένη	Υψηλή
Τέλη συναλλαγών	Συνήθως υπάρχουν	Πολύ χαμηλά ή μηδενικά
Καταλληλότητα για IoT	Μέτρια	Υψηλή
Παράδειγμα	Bitcoin	IOTA / Shimmer



Εικόνα 4.8 Το 4.8α δείχνει την τοπολογία Tangle, ενώ το 4.8β δείχνει την τοπολογία blockchain. Πηγή: Sealey et al (2022).

Χαρακτηριστικό	Blockchain	DAG	IOTA/Shimmer
Δομή ledger	Linear chain	DAG	Tangle
Παράλληλες συναλλαγές	Περιορισμένες	Ναι	Ναι
Blocks	Ναι	Εξαρτάται	DAG blocks
Fees	Εξαρτάται	Εξαρτάται	Feeless L1

Χαρακτηριστικό	Blockchain	DAG	IOTA/Shimmer
IoT suitability	Μέτρια	Υψηλή	Υψηλή
Smart contracts	Ναι	Εξαρτάται	μέσω L2
Tokenization	Εξαρτάται	Εξαρτάται	Stardust



Εικόνα 4.9 Απεικόνιση (α) ενός παραδοσιακού blockchain, (β) του IOTA Tangle και (γ) της αρχιτεκτονικής ISCP δύο επιπέδων όπου επισημαίνονται δύο πιθανές αλυσίδες αγκυρωμένες σε διαφορετικούς κόμβους πίνακα. Πηγή: Keramat et al. (2022)

Κεφάλαιο 5ο: Πρωτόκολλα Συναίνεσης

5.1 Πρωτόκολλα Συναίνεσης

Από την έναρξη του Bitcoin, τα κρυπτονομίσματα και η υποκείμενη τεχνολογία blockchain έχουν προσελκύσει αυξανόμενο ενδιαφέρον τόσο από τον ακαδημαϊκό χώρο όσο και από τη βιομηχανία. Μεταξύ διαφόρων βασικών συνιστωσών, το πρωτόκολλο συναίνεσης (δηλαδή πώς να επιτευχθεί συμφωνία μεταξύ ενός κατακευματισμένου δικτύου κόμβων), είναι η καθοριστική τεχνολογία πίσω από την ασφάλεια και την απόδοση του blockchain (Bano et al. 2019, Xiao et al. 2020).

Ένα blockchain είναι ένα κατακευματισμένο βιβλίο καταγραφής συναλλαγών, το οποίο διατηρείται από πολλούς κόμβους χωρίς κεντρική εξουσία, μέσω ενός κατακευματισμένου κρυπτογραφικού πρωτοκόλλου. Όλοι οι κόμβοι επικυρώνουν τις πληροφορίες που πρόκειται να προστεθούν στο blockchain και ένα πρωτόκολλο συναίνεσης διασφαλίζει ότι οι κόμβοι συμφωνούν σε μια μοναδική σειρά με την οποία προστίθενται οι καταχωρήσεις. Τα πρωτόκολλα συναίνεσης σε ορισμένες πλατφόρμες blockchain περιλαμβάνουν τα Hyperledger Fabric, Tendermint, Symbiont, R3~Corda, Iroha, Kadena, Chain, Quorum, MultiChain, Sawtooth Lake, Ripple, Stellar και IOTA (Cachin and Vukolić 2017).

Οι μηχανισμοί συναίνεσης έχουν ενσωματωθεί στις αλυσίδες μπλοκ ως μηχανισμός ανοχής σφαλμάτων για την επαλήθευση συναλλαγών. Η συναίνεση χρησιμοποιείται για τη διατήρηση της συμφωνίας μεταξύ των κόμβων στο δίκτυο, διότι όταν το δίκτυο επεκτείνεται, και ο αριθμός των κόμβων αυξάνεται, είναι αρκετά δύσκολο να επιτευχθεί συμφωνία. Το δημόσιο blockchain απαιτεί τη συμμετοχή χρηστών για την επαλήθευση και τον έλεγχο ταυτότητας των συναλλαγών. Επειδή το blockchain είναι ένα δυναμικό, αυτορρυθμιζόμενο σύστημα, απαιτείται η ενσωμάτωση ενός ασφαλούς μηχανισμού για να διασφαλίσει την αυθεντικότητα των συναλλαγών, με το δεδομένο ότι οι συμμετέχοντες έχουν καταλήξει σε συμφωνία για συναίνεση. Έχουν προταθεί διάφοροι τύποι μηχανισμών συναίνεσης οι οποίοι διαφέρουν μεταξύ τους ως προς τις βασικές αρχές και εφαρμογές τους (Lashkari and Musilek 2021).

Η πρωτοποριακή εργασία των Dwork, Lynch και Stock το 1988 (Xiao et al. 2020), έθεσε τα θεωρητικά θεμέλια της μερικώς σύγχρονης συναίνεσης. Αναλύοντας τον στόχο της συναίνεσης σε τερματισμό και ασφάλεια, οι συγγραφείς μπόρεσαν να αποδείξουν επίσημα τη σκοπιμότητα τεσσάρων στόχων συναίνεσης, συμπεριλαμβανομένων των CFT, ανοχής παράλειψης, BFT, μη αυθεντικοποιημένου BFT, υπό την συνθήκη συγχρονισμού/τελικού συγχρονισμού.

5.2 Συναίνεση σε κλασικά blockchain

Ο στόχος ενός πρωτοκόλλου συναίνεσης blockchain είναι να διασφαλίσει ότι όλοι οι συμμετέχοντες κόμβοι συμφωνούν σε ένα κοινό ιστορικό συναλλαγών δικτύου, το οποίο σειριοποιείται με τη μορφή blockchain. Για τη συναίνεση blockchain ορίζονται οι εξής απαιτήσεις: α) Λήξη Σε κάθε ειλικρινή κόμβο, μια νέα συναλλαγή είτε απορρίπτεται είτε γίνεται δεκτή, β) Συμφωνία Κάθε νέα συναλλαγή και το μπλοκ που την κρατάει θα πρέπει είτε να γίνονται δεκτά, είτε να απορρίπτονται από όλους τους κόμβους. γ) Εγκυρότητα Εάν κάθε κόμβος λάβει την ίδια έγκυρη συναλλαγή, θα πρέπει να γίνεται δεκτό στο blockchain. δ) Ακεραιότητα Σε κάθε ειλικρινή κόμβο, όλες οι αποδεκτές συναλλαγές θα πρέπει να είναι συνεπείς μεταξύ τους (χωρίς διπλές δαπάνες). Όλα τα αποδεκτά μπλοκ θα πρέπει να δημιουργούνται σωστά και να συνδέονται με αλυσίδα κατακευματισμού σε χρονολογική σειρά. Αυτές οι απαιτήσεις μπορούν να χρησιμεύσουν ως οι αρχές σχεδιασμού νέων πρωτοκόλλων blockchain (Cachin and Vukolić 2017).

Ένα πρωτόκολλο συναίνεσης συγκεντρώνει πέντε βασικά στοιχεία (Xiao et al. 2020).

- Πρόταση μπλοκ: Δημιουργία μπλοκ και επισύναψη αποδείξεων δημιουργίας.
- Διάδοση πληροφοριών: Διάδοση μπλοκ και συναλλαγών σε όλο το δίκτυο.
- Επικύρωση μπλοκ: Έλεγχος μπλοκ για αποδείξεις δημιουργίας και εγκυρότητα συναλλαγής.
- Οριστικοποίηση μπλοκ: Επίτευξη συμφωνίας σχετικά με την αποδοχή επικυρωμένων μπλοκ.
- Μηχανισμός κινήτρων: Προώθηση της ειλικρινούς συμμετοχής και δημιουργία διακριτικών δικτύου.

Αν και τα πέντε στοιχεία θεωρούνται σημαντικά για την επιτυχή συναίνεση για το blockchain, ένα πρωτόκολλο συναίνεσης blockchain μπορεί να μην τα καλύπτει όλα (Xiao et al. 2020).

Το πρόβλημα της καταναεμημένης συναίνεσης με ανοχή σφαλμάτων (FT) έχει μελετηθεί εκτενώς σε καταναεμημένα συστήματα από τα τέλη της δεκαετίας του 1970 και τελευταία απέκτησε μεγαλύτερη σημασία για την τεχνολογία blockchain, ειδικά για τα blockchain με άδεια, όπου κάθε συμμετέχων σε συναίνεση αποκαλύπτει την ταυτότητά του. Ανάλογα με το μέσο ανταλλαγής μηνυμάτων, τα καταναεμημένα συστήματα ταξινομούνται σε δύο τύπους: μετάδοση μηνυμάτων και κοινόχρηστη μνήμη. Τα συστήματα μετάδοσης μηνυμάτων παρουσιάζουν ομοιότητα με τα σύγχρονα συστήματα blockchain, όπου η καταναεμημένη συναίνεση σε ένα μοναδικό ιστορικό δικτύου επιτυγχάνεται μέσω επικοινωνίας peer-to-peer. Τα παραδοσιακά πρωτόκολλα blockchain, όπως η συναίνεση Nakamoto (2008), οργανώνουν μπλοκ συναλλαγών διαδοχικά σε μια αλυσίδα, όπου κάθε μπλοκ αναφέρεται στον προκάτοχό του, επεκτείνοντας πίσω στο μπλοκ γένεσης. Η συναίνεση σε αυτά τα συστήματα συχνά προχωρά σε γύρους, με νέα μπλοκ να προστίθενται στη μεγαλύτερη αλυσίδα, την οποία οι συμμετέχοντες αναγνωρίζουν ως το έγκυρο καθολικό. Αυτή η γραμμική δομή, ωστόσο, επιβάλλει περιορισμούς στην επεκτασιμότητα και την απόδοση. Το πρωτόκολλο συναίνεσης Nakamoto (2008) είναι το πρωτόκολλο που εφαρμόζεται στο δίκτυο Bitcoin. Με τη βοήθεια αυτού του πρωτοκόλλου συναίνεσης, το Bitcoin έγινε το πρώτο σύστημα ψηφιακού νομίσματος που αντιστάθηκε σε επιθέσεις διπλής δαπάνης σε ένα αποκεντρωμένο δίκτυο peer-to-peer με περιορισμένη εμπιστοσύνη. Καθώς το δίκτυο Bitcoin συνεχίζει να αναπτύσσεται, το πρωτόκολλο συναίνεσης Nakamoto έχει αντιμετωπίσει αρκετά σημεία συμφόρησης στην απόδοση και προβλήματα βιωσιμότητας. Ερευνητές σε κοινότητες blockchain έχουν εκφράσει ανησυχίες σχετικά με το πρωτόκολλο συναίνεσης Nakamoto και ιδιαίτερα τον μηχανισμό που βασίζεται σε PoW (απόδειξη Εργασίας), όσον αφορά την κατανάλωση ενέργειας (μη βιώσιμη), την χωρητικότητα συναλλαγών και την επεκτασιμότητα (χαμηλή χωρητικότητα συναλλαγών και κακή επεκτασιμότητα). Επιπλέον εκφράζονται ανησυχίες για την ασφάλεια μακροπρόθεσμα (Xiao et al, 2020). Από τότε που προτάθηκε το blockchain, έχουν διεξαχθεί πολλές έρευνες για την αντιμετώπιση των ελλείψεων του blockchain, όπως ο περιορισμός του σε όλη του την έκταση. Το blockchain που βασίζεται σε DAG προτάθηκε ως η επόμενη γενιά του blockchain. Το ημερολόγιο που βασίζεται σε άμεσο ακυκλικό γράφημα (DAG) και ο αντίστοιχος αλγόριθμος συναίνεσης έχουν αναγνωριστεί ως μια πολλά υποσχόμενη τεχνολογία για το Διαδίκτυο των Πραγμάτων (IoT). Σε σύγκριση με την Απόδειξη Εργασίας (PoW) και την Απόδειξη Συμμετοχής (PoS) που έχουν χρησιμοποιηθεί ευρέως στο blockchain, ο μηχανισμός συναίνεσης που έχει σχεδιαστεί για τη δομή DAG (συναίνεση DAG) μπορεί να ξεπεράσει ορισμένες αδυναμίες, όπως η υψηλή κατανάλωση ενέργειας, το υψηλό τέλος συναλλαγής, η χαμηλή απόδοση συναλλαγής και η μεγάλη καθυστέρηση επιβεβαίωσης (Li et al. 2020).

Οι Belotti et al. (2019) παρέχουν έναν οδηγό για την τεχνολογία blockchain, Υπάρχουν συμπεριλαμβανομένου του ιστορικού ανάπτυξης, της δομής συναλλαγών και του καθολικού μητρώου, της αφαίρεσης του συστήματος blockchain, των μηχανισμών συναίνεσης και ενός λεπτομερούς οδηγού για το πότε και πώς και ποια τεχνολογία blockchain να χρησιμοποιήσει κάποιος. Οι Xiao et al. (2019) περιγράφουν συνοπτικά διάφορα καταναεμημένα πρωτόκολλα συναίνεσης, από τα κλασικά πρωτόκολλα BFT (Βυζαντινή Συναίνεση σε Σφάλματα), έως το πρωτόκολλο συναίνεσης Nakamoto, καθώς και νεότερες ανακαλύψεις στη συναίνεση για το blockchain. Ειδικότερα, παρέχουν μια

περίληψη των στόχων συναίνεσης για blockchain χωρίς άδεια, ακολουθώντας το παράδειγμα της κλασικής συναίνεσης με βάση το BFT (Βυζαντινή Συναίνεση σε Σφάλματα). Οι μηχανισμοί συναίνεσης που καλύπτονται περιλαμβάνουν αλγόριθμους PoW, PoS, BFT και υβριδικούς αλγόριθμους που βασίζονται στο BFT. Υπάρχουν τρεις κατηγορίες πρωτοκόλλων συναίνεσης που βασίζονται στον σχηματισμό επιτροπών και στους κανόνες πρότασης μπλοκ: (i) πρωτόκολλα που βασίζονται στην απόδειξη εργασίας PoW, (ii) πρωτόκολλα απόδειξης X που αντικαθιστούν την απόδειξη εργασίας με πιο ενεργειακά αποδοτικές εναλλακτικές λύσεις X (PoX) για το PoW και (iii) υβριδικά πρωτόκολλα που είναι συνθέσεις ή παραλλαγές των κλασικών πρωτοκόλλων συναίνεσης (Bano et al. 2019).

5.3 Γιατί τα DAG χρειάζονται διαφορετική προσέγγιση όσον αφορά τα πρωτόκολλα συναίνεσης

Τα πρωτόκολλα συναίνεσης που βασίζονται σε DAG επιτρέπουν στα μπλοκ να αναφέρουν πολλαπλούς προκατόχους, δημιουργώντας μια δομή Κατευθυνόμενου Ακυκλικού Γραφήματος (DAG). Αυτός ο μηχανισμός αναφοράς επιτρέπει ένα πλαίσιο όπου μπορούν να προστεθούν ταυτόχρονα πολλαπλά μπλοκ, υποστηρίζοντας την παράλληλη επεξεργασία συναλλαγών. Στην επιδίωξη της περίπλοκης ισορροπίας μεταξύ ασφάλειας και απόδοσης, προτάθηκαν πρωτόκολλα συναίνεσης που βασίζονται σε DAG ως λύση. Τα πρωτόκολλα αυτά προσφέρουν βελτιωμένη επεκτασιμότητα, ευελιξία και γρήγορη επιβεβαίωση συναλλαγών (Raikwar, et al. 2025). Τα πλεονεκτήματα των πρωτοκόλλων συναίνεσης που βασίζονται σε DAG σε σύγκριση με τα blockchains, τα πρωτόκολλα γραμμικής αλυσίδας, είναι τα ακόλουθα (Raikwar, et al. 2025):

1.Επεκτασιμότητα: Τα πρωτόκολλα που βασίζονται σε DAG μπορούν να επεξεργάζονται συναλλαγές παράλληλα και όχι διαδοχικά, με αποτέλεσμα τη βελτιωμένη επεκτασιμότητα και απόδοση σε σύγκριση με τα διαδοχικά blockchains.

2. Λανθάνουσα κατάσταση: Ο βαθμός στον οποίο τα πρωτόκολλα που βασίζονται σε DAG μειώνουν την καθυστέρηση εξαρτάται από την συγκεκριμένη προσέγγιση και τις αρχιτεκτονικές αποφάσεις γύρω από τον συγχρονισμό και την ασφάλεια. Για παράδειγμα στα πρωτόκολλα που βασίζονται σε PoW (Απόδειξη Εργασίας), μια δομή DAG επιτρέπει ταχύτερη επιβεβαίωση συναλλαγών, ενώ σε ορισμένα πρωτόκολλα που βασίζονται σε Απόδειξη Συμμετοχής (Proof of Stake PoS), η χρήση πρόσθετων αξιόπιστων πρωτότυπων μετάδοσης αυξάνει την καθυστέρηση.

3. Ευελιξία: Η αρχιτεκτονική DAG είναι ενδεχομένως πιο ευέλικτη από ένα blockchain. Ενώ στα παραδοσιακά blockchains, κάθε μπλοκ εξυπηρετεί τρεις ρόλους, ενεργεί ως ηγέτης που επικυρώνει τις συναλλαγές, παρέχει περιεχόμενο με τη μορφή δεδομένων συναλλαγών και ψηφίζει για το ιστορικό αιτιών, τα μπλοκ σε μια δομή DAG μπορούν να έχουν διαφοροποιημένους ρόλους, επιτρέποντας μια πιο κατανεμημένη προσέγγιση στη συναίνεση και την επικύρωση συναλλαγών. Αποτέλεσμα αυτού είναι να επιτρέπει πιο ευέλικτους μηχανισμούς συναίνεσης και να μπορεί να προσαρμοστεί σε διάφορες συνθήκες δικτύου.

4. Παράλληλη εγγραφή: Τα πρωτόκολλα που βασίζονται σε DAG επιτρέπουν την ταυτόχρονη παραγωγή μπλοκ, αποκλίνοντας από το μοντέλο δημιουργίας μπλοκ που βασίζεται σε οδηγούς των παραδοσιακών blockchain. Αυτή η αρχιτεκτονική επιτρέπει σε πολλαπλούς συμμετέχοντες να προσθέτουν ταυτόχρονα συναλλαγές, διευρύνοντας αποτελεσματικά την πρόσβαση εγγραφής. Στην πιο ακραία περίπτωση, κάθε συμμετέχων μπορεί να παράγει ανεξάρτητα μπλοκ, εξαλείφοντας την εξάρτηση από έναν μόνο ή μια ομάδα παραγωγών μπλοκ. Αυτή η ιδιότητα μπορεί να μειώσει την καθυστέρηση και να εξαλείψει τα σημεία συμφόρησης που σχετίζονται με τη διαδοχική δημιουργία μπλοκ (Raikwar, et al. 2025).

5.4 Συμβουλές για την επιλογή του πρωτοκόλλου συναίνεσης

Το πρόβλημα συναίνεσης προκύπτει παραδοσιακά και σε τεχνικά συστήματα για την παρακολούθηση αντικειμένων, την ταξινόμηση πυκνότητας, τη σύντηξη αισθητήρων [4], τον εντοπισμό ρομπότ και τον σχεδιασμό αποστολών. Επιπλέον, η συλλογική και κατανεμημένη λήψη αποφάσεων είναι σημαντική στην κοινωνική δυναμική. Το πρόβλημα συναίνεσης βρίσκεται επίσης στην καρδιά της τεχνολογίας κατανεμημένου καθολικού [9], καθώς επιτρέπει την επίτευξη συναίνεσης σχετικά με το εάν θα προστεθεί μια συναλλαγή σε ένα καθολικό ή θα συμφωνηθεί μια χρονική σήμανση μιας συναλλαγής. Κάθε κόμβος σε ένα κατανεμημένο σύστημα συναίνεσης ακολουθεί απλούς κανόνες, χρησιμοποιώντας μόνο τοπικές πληροφορίες και επικοινωνία μεταξύ κόμβων. Οι αλγόριθμοι που εκτελούν τέτοιες εργασίες θα πρέπει να είναι ανθεκτικοί σε διαφορετικούς τύπους διαταραχών και βυζαντινών ρυθμίσεων. Η μελέτη-ορόσημο των Pease et al. το 1980 εξετάζει την ανθεκτικότητα της συναίνεσης με ελαττωματικούς κόμβους. Συγκεκριμένα, οι Pease et al. (1980) έδειξαν ότι για σύγχρονα συστήματα, απαραίτητη προϋπόθεση για την επίτευξη συναίνεσης είναι να είναι ελαττωματικοί το πολύ το 1/3 των κόμβων. Στη σημαντική εργασία των Fischer et al. (1985) αυτό το αποτέλεσμα ενισχύεται με την έννοια ότι, σε ασύγχρονες καταστάσεις ήδη, μόνο ένας ελαττωματικός κόμβος μπορεί να αποτρέψει μια συμφωνία (Carpossele, et al. 2021),

Στην εργασία τους οι Carpossele, et al. (2021), συνέκριναν πρωτόκολλα συναίνεσης δυαδικής πλειοψηφίας χωρίς οδηγό σε διάφορες ελαττωματικές και βυζαντινές υποδομές. Εστίασαν σε ένα νέο γρήγορο πιθανοτικό πρωτόκολλο συναίνεσης χωρίς ηγέτη FPC-BI: Γρήγορη Πιθανοτική Συναίνεση εντός Βυζαντινών Υποδομών) με χαμηλή επικοινωνιακή πολυπλοκότητα και το οποίο επιτρέπει σε ένα σύνολο κόμβων να καταλήξουν σε συναίνεση για την τιμή ενός μόνο bit (Poron and Buchanan 2021). Σε αυτό το πρωτόκολλο, προστίθεται τυχαιότητα σε ένα πρωτόκολλο συναίνεσης τυχαίας πλειοψηφίας προκειμένου να βελτιωθεί η απόδοση παρουσία βυζαντινών δρώντων. Εισήγαγαν τοπικούς κανόνες διακοπής για να επιτρέψουν στους κόμβους να ολοκληρώνουν μεμονωμένα και αυτόματα. Επιπλέον, το όριο για την πλειοψηφία στον πρώτο γύρο εφαρμόζεται σε μια σταθερή τιμή $>0,5$ για να υποστηρίξει την ασύμμετρη σημασία της ακεραιότητας 0 και 1. Όρισαν αρκετές στρατηγικές αντιπαράθεσης για να αναλύσουν την απόδοση του πρωτοκόλλου σε βυζαντινό περιβάλλον. Ένας αντίπαλος μπορεί να είναι προσεκτικός απαντώντας στον ίδιο γύρο με την ίδια γνώμη σε όλους, ή Berserk απαντώντας σε διαφορετικά ερωτήματα με διαφορετικές απόψεις. Αν και το τελευταίο μπορεί να είναι ανιχνεύσιμο, υποθέτουμε σε αυτή την εργασία ότι δεν εφαρμόζεται τέτοιος μηχανισμός ανίχνευσης στο πρωτόκολλο για να αποδυναμώσει ή να αποτρέψει μια επίθεση Berserk. Κατά συνέπεια, η επίθεση Berserk μπορεί να οδηγήσει σε πιο συχνές αποτυχίες συμφωνίας ή τερματισμού. Χρησιμοποίησαν εργαλεία προσομοίωσης για να μελετήσουν και να αξιολογήσουν την απόδοση του πρωτοκόλλου με υψηλή στατιστική σημαντικότητα. Προς τον σκοπό αυτό, μελέτησαν τον ρυθμό με τον οποίο το πρωτόκολλο ολοκληρώνεται με επιτυχία. Αυτό μετρήθηκε σε σχέση με τρεις τύπους αστοχιών: συμφωνία, τερματισμό και αποτυχία ακεραιότητας. Για το τελευταίο, γίνεται διάκριση μεταξύ αποτυχίας ακεραιότητας 0 και 1. Σε διάφορες πραγματικές καταστάσεις, οι κόμβοι ενδέχεται να μην έχουν πλήρη εικόνα δικτύου. Το πρωτόκολλο μελετάται όταν οι κόμβοι είναι ικανοί να υποβάλλουν ερωτήματα μόνο σε μέρη του δικτύου. Για να το γίνει αυτό, χρησιμοποιήθηκε ένα μοντέλο WattsStrogatz για να δημιουργήσουν ένα γράφημα με τις ακμές που συνδέουν κόμβους που μπορούν να υποβάλλουν ερωτήματα ο ένας στον άλλον. Μια μερική εικόνα δικτύου περίπου 50% είναι επαρκής αν ληφθεί υπόψη η συντηρητική περίπτωση ενός δακτυλιοειδούς γραφήματος. Εάν ορισμένες από τις συνδέσεις στο δακτυλιοειδές γράφημα επανασυνδεθούν τυχαία, το πρωτόκολλο αποδίδει καλά με πολύ μικρότερη αντίληψη δικτύου ανά κόμβο. Υπέθεσαν ότι η πιο συντηρητική περίπτωση για την 0- Γνώμη είναι 49%. Έδειξαν ότι υπάρχει ανταγωνισμός μεταξύ της διασφάλισης

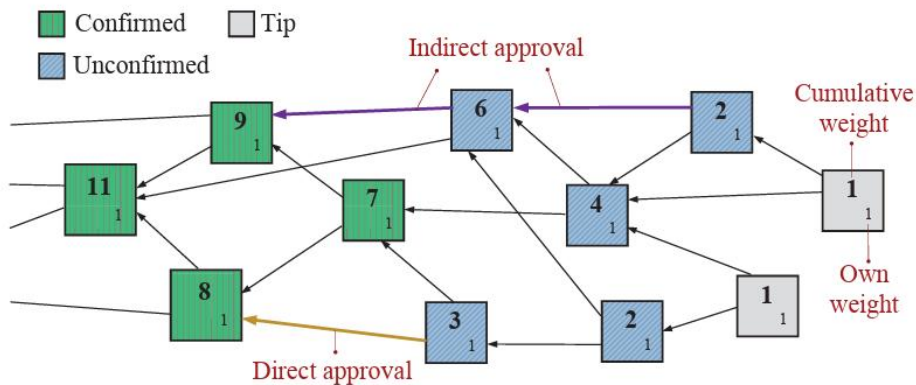
του ρυθμού ακεραιότητας 0 και 1. Αν και έθεσαν την πιο συντηρητική περίπτωση για την ακεραιότητα 0, το πρωτόκολλο μπορεί να αποτρέψει και τις δύο αποτυχίες ακεραιότητας εάν ο αντίπαλος έχει έως και 10% έλεγχο στο δίκτυο.

Η απόδοση του πρωτοκόλλου βελτιώθηκε με την αύξηση του μεγέθους της απαρτίας και αρκούσε να υποβληθεί ερώτημα σε ένα κλάσμα των κόμβων για να αποφευχθεί μια αποτυχία ακεραιότητας. Διερεύνησαν την απόδοση του πρωτοκόλλου όταν το δίκτυο κλιμακώνεται και φάνηκε ότι το πρωτόκολλο απέδιδε παρόμοια με τις ίδιες ρυθμίσεις παραμέτρων ανά κόμβο. Επίσης ανάλογα με την εφαρμογή μπορεί να είναι απαραίτητο να μειωθεί το εύρος του τυχαίου κατώφλιου, καθώς το πρωτόκολλο μπορεί να αντέξει μεγαλύτερο αριθμό τυχαίων κόμβων όταν το κατώφλι παραμένει κοντά στο 0,5. Ανέλυσαν το ποσοστό τερματισμού και συμφωνίας του πρωτοκόλλου για μια προσεκτική και Berserk Byzantine στρατηγική και για μια αρχική ρύθμιση χειρότερης περίπτωσης. Έδειξαν ότι το πρωτόκολλο μπορεί να αποτραπεί από το να τερματιστεί και να καταλήξει σε συμφωνία για μεγάλο χρονικό διάστημα και ότι η εισαγωγή της τυχειότητας μειώνει δραστικά τις επιπτώσεις αυτής της επίθεσης. Επίσης ότι για το ίδιο ποσοστό αντίπαλων κόμβων η στρατηγική Berserk είναι σημαντικά πιο σοβαρή από την προσεκτική στρατηγική και μπορεί να φτάσει σε αποτυχία συμφωνίας πολύ πιο αποτελεσματικά. Έδειξαν τέλος ότι, όπως ένα δίκτυο που καταλαμβάνεται μόνο από έντιμους δράστες, το πρωτόκολλο αποδίδει καλά εάν κάθε κόμβος έχει μόνο μια εικόνα του δικτύου περίπου 50%. Γενικά, το πρωτόκολλο φαίνεται ευαίσθητο στην εξάπλωση των τυχαίων κατωφλίων και υπάρχει ένα βέλτιστο σύνολο παραμέτρων. Από την άλλη πλευρά, δεν είναι απαραίτητο οι κόμβοι να λαμβάνουν έναν τυχαίο αριθμό για το τυχαίο κατώφλι σε κάθε γύρο, καθώς η απόδοση του πρωτοκόλλου παραμένει η ίδια ακόμη και αν εφαρμόζεται περιστασιακά ένας κανόνας απλής πλειοψηφίας (Caroselle, et al. 2021). Οι Rochman et al. (2023), πρότειναν έναν αλγόριθμο βελτιστοποίησης επιλογής συμβουλών που βασίζεται στο WRW με δυναμικό άλφα, ο οποίος ονομάζεται DA-IOTA. Αυτή η προσέγγιση χρησιμοποιείται για την υπερνίκηση των συμβουλών που καθυστερούν και τη διατήρηση υψηλού επιπέδου εμπιστοσύνης στο μπλέξιμο χρησιμοποιώντας μεθόδους, δίνοντας προτεραιότητα στην ισορροπία της τυχειότητας έναντι της αβεβαιότητας τυχειότητας όπως το E-IOTA. Η θεμελιώδης διαφορά από τη μέθοδο E-IOTA είναι ότι η μέθοδος χρησιμοποιεί άλφα τυχαία με βάση τρεις προκαθορισμένες τιμές πιθανότητας, ενώ το DA-IOTA χρησιμοποιεί την τυπική απόκλιση του εγκρίνοντος για τον προσδιορισμό του άλφα. Το επίπεδο εμπιστοσύνης υποδεικνύει πόσο πιθανό είναι οι νέες εισερχόμενες συναλλαγές να αποδεχτούν τη συναλλαγή. Όσο περισσότερες συναλλαγές μπορεί να αποδεχτεί μια νέα συναλλαγή, τόσο υψηλότερη είναι η εμπιστοσύνη σε αυτήν τη συναλλαγή. Με πρόσθετες επιβεβαιώσεις, το σωρευτικό βάρος κάθε συναλλαγής αυξάνεται. Αυτό καθιστά πιο επικερδή την επιλογή αυτής της επιχείρησης στο μέλλον, επομένως η σύγχυση είναι ότι πιστεύεται ότι είναι υψηλή. Αυτό βοηθά στη διασφάλιση ασφαλέστερης εμπλοκής καθοδηγώντας τον χρήστη να επιλέξει το πιο πιθανό συμβάν μεταξύ δύο αντικρουόμενων συμβάντων. Οι συναλλαγές όπου γίνεται προσπάθεια να ξοδευτούν τα ίδια χρήματα πολλές φορές (το λεγόμενο διπλό κόστος) είναι μια συναλλαγή σύγκρουσης. Ωστόσο, μόνο ένα αντίθετο συμβάν θα εγκριθεί ως πραγματικό συμβάν, ενώ τα άλλα αγνοούνται. Η θεμελιώδης ιδέα του DA-IOTA είναι το δυναμικό άλφα σε κάθε βήμα του WRW χρησιμοποιώντας την τυπική απόκλιση όλων των αθροιστικών βαρών έγκρισης για τον προσδιορισμό του μεγέθους του άλφα. Το μέγεθος του άλφα θα καθορίσει το επίπεδο τυχειότητας της πιθανότητας επιλογής συμβουλής. Αυτό το άλφα χρησιμοποιείται στη συνέχεια για τον υπολογισμό της πιθανότητας συναλλαγής.

5.5 FPC / συναίνεση πιθανοτήτων

Σύμφωνα με τους Lin et al. (2022) το πρωτόκολλο συναίνεσης Tangle 2.0 σε ένα βυζαντινό περιβάλλον, είναι ανθεκτικό στην επίθεση δόλωμα-και-αλλαγή έως το θεωρητικό ανώτερο όριο του 33% του βάρους ψήφου του αντιπάλου. Ο μηχανισμός κοινού νομίσματος στο Tangle 2.0 είναι απαραίτητος για την ανθεκτικότητα έναντι ισχυρών αντιπάλων. Επιπλέον, τα πειραματικά τους αποτελέσματα επιβεβαιώνουν ότι το πρωτόκολλο μπορεί να επιτύχει χρόνο επιβεβαίωσης περίπου 1 δευτερολέπτου σε τυπικά σενάρια και ότι οι χρόνοι επιβεβαίωσης των μη συγκρουόμενων συναλλαγών δεν επηρεάζονται από την παρουσία συγκρούσεων. Το πρωτόκολλο συναίνεσης Tangle 2.0 αποτελείται από δύο στοιχεία: το ασύγχρονο στοιχείο, On Tangle Voting (OTV), και το σύγχρονο μέρος, Synchronised Random Reality Selection (SRRS). Για να διερευνηθεί η ασφάλεια αυτών των στοιχείων, εισάγεται στις προσομοιώσεις μια στρατηγική επίθεσης που βασίζεται σε πράκτορες, που ονομάζεται Bait-and-Switch. Σε αυτό το είδος επίθεσης, οι αντίπαλοι μπορούν να εκδώσουν διπλές δαπάνες σε αυθαίρετη υψηλή συχνότητα και να στοχεύσουν να διατηρήσουν τους ειλικρινείς κόμβους σε μια αναποφάσιστη κατάσταση. Τα αποτελέσματα της προσομοίωσης έδειξαν ότι στην περίπτωση της χειρότερης κατανομής βάρους, όπου όλοι οι ειλικρινείς κόμβοι έχουν ίσο βάρος, το πρωτόκολλο OTV μπορεί ακόμα να αντισταθεί στην επίθεση Bait-and-Switch όταν ο αντίπαλος κόμβος κατέχει έως και 20% του συνολικού βάρους. Επιπλέον, έδειξαν ότι το πρωτόκολλο SRRS μπορεί περαιτέρω να αντισταθεί στην επίθεση Bait-and-Switch, ακόμη και όταν ο αντίπαλος καταλαμβάνει έως και 33% του συνολικού βάρους, που είναι ο θεωρητικός άνω δεσμός.

Εκτός από αυτά τα αποτελέσματα, η τυχαιοποίηση στο πρωτόκολλο FPC χρησιμεύει ως «ομίχλη πολέμου», για πιθανούς κακόβουλους εισβολείς, καθιστώντας στην καλύτερη περίπτωση αδύνατο για τον εισβολέα να ελέγξει τους ειλικρινείς κόμβους. Ωστόσο, αξ σημειώσουμε ότι η πρόσθετη τυχαioτητα μπορεί να έχει ορισμένες αρνητικές παρενέργειες: μπορεί να καθυστερήσει τον τερματισμό του πρωτοκόλλου και να μειώσει το ποσοστό ακεραιότητας. Το FPC περιέχει δύο επιπλέον νέα χαρακτηριστικά σε σύγκριση με τους προκατόχους του. Πρώτον, οι κόμβοι ακολουθούν έναν τοπικό κανόνα διακοπής σχετικά με το πότε πρέπει να σταματήσουν να υποβάλλουν ερωτήματα σε άλλους κόμβους. Μόλις όλοι οι κόμβοι σταματήσουν να υποβάλλουν ερωτήματα, το πρωτόκολλο τερματίζεται αυτόματα. Δεύτερον, το πρωτόκολλο είναι ασύμμετρο με την έννοια, ότι οι δύο δυαδικές επιλογές, 0 και 1, δεν χρειάζεται να έχουν την ίδια σημασία. Για παράδειγμα, σε διάφορες εφαρμογές, μπορεί να είναι σκόπιμο να γίνει διάκριση μεταξύ των ακόλουθων δύο διαφορετικών ειδών σφαλμάτων. Εάν δηλαδή αρχικά, η πλειοψηφία των κόμβων προτιμά το 0, αλλά το τελικό αποτέλεσμα του πρωτοκόλλου είναι 1, και από την άλλη πλευρά, εάν η πλειοψηφία των κόμβων προτιμά αρχικά το 1, αλλά το τελικό αποτέλεσμα του πρωτοκόλλου είναι 0. Αυτή η διάκριση μεταξύ των διαφορετικών ειδών σφαλμάτων είναι μια τυπική προσέγγιση στη θεωρία στατιστικών δοκιμών και στην αξιολόγηση των δυαδικών ταξινομητών. Τα δύο διαφορετικά είδη σφαλμάτων ενός δυαδικού κανόνα απόφασης ή ταξινομητή μετρώνται διαφορετικά σε διαφορετικά πεδία. Για παράδειγμα, στην ιατρική, η ευαισθησία και η εξειδίκευση χρησιμοποιούνται συχνά, στη στατιστική θεωρία δοκιμών, γίνεται λόγος για σφάλματα τύπου I και τύπου II, και στην επιστήμη των υπολογιστών, προτιμώνται η ακρίβεια και η ανάκληση. Στα μελετώμενα πρωτόκολλα οι κόμβοι χρησιμοποιούν μόνο τοπικές πληροφορίες στο δίκτυο, επιτρέποντας στο πρωτόκολλο να εκτελείται σε δίκτυα χωρίς άδεια. Επιπλέον, δεν υπάρχει κεντρική οντότητα ή εκλεγμένος ηγέτης που να «επιβλέπει» το δίκτυο και να αποφασίζει εάν επιτεύχθηκε συναίνεση. Η έλλειψη μιας τέτοιας οντότητας σημαίνει ότι κάθε κόμβος πρέπει να αποφασίσει πότε θα σταματήσει να χρησιμοποιεί έναν τοπικό κανόνα, δηλαδή, να χρησιμοποιεί μόνο τις πληροφορίες που είναι τοπικά διαθέσιμες σε αυτόν (Capocelle et al. 2021).



Εικόνα 5.1 Παράδειγμα διαδικασίας συναίνεσης στο Tangle Πηγή: Li et al. (2020)

5.6 Byzantine Fault Tolerance και DAG

Οι Cachin and Vukolić, (2017) παρέχουν μια επισκόπηση δεκατριών εξεχόντων πρωτοκόλλων συναίνεσης που έχουν σχεδιαστεί για πλατφόρμες blockchain με άδεια, μαζί με τις ιδιότητες ανοχής σφαλμάτων και ασφάλειας που προσφέρουν. Ένα ευρύ φάσμα πρωτοκόλλων συναίνεσης blockchain έχει προταθεί, συνοδευόμενο από αλγοριθμικές αφαιρέσεις και αναλύσεις τρωτότητας (Xiao et al. 2020). Με βάση το πρόβλημα των Βυζαντινών Γενικών, τα σφάλματα σε ένα καταναμημένο δίκτυο μπορούν να χωριστούν σε δύο κατηγορίες: σφάλματα κατάρρευσης και Βυζαντινά σφάλματα.

- Τα σφάλματα κατάρρευσης ονομάζονται επίσης μη Βυζαντινά σφάλματα. Προκύπτουν από σφάλματα όπως καθυστέρηση και απώλεια και δεν προκαλούν άλλες κακόβουλες ενέργειες. Αυτός ο τύπος σφάλματος είναι ο πιο βασικός και συνηθισμένος τύπος που πρέπει να λυθεί σε καταναμημένα συστήματα. Οι μηχανισμοί συναίνεσης που αντιμετωπίζουν μόνο αυτόν τον τύπο σφάλματος ονομάζονται ανοχή σφάλματος κατάρρευσης (CFT) μηχανισμοί συναίνεσης (Cachin and Vukolić 2017).

- Τα Βυζαντινά σφάλματα μπορούν να προκαλέσουν κακόβουλες ενέργειες, όπως σκόπιμη καθυστέρηση μηνυμάτων και εξαπάτηση άλλων κόμβων. Αυτός ο τύπος σφάλματος είναι πιο περίπλοκος στην αντιμετώπιση. Οι μηχανισμοί συναίνεσης που αντιμετωπίζουν αυτόν τον τύπο σφάλματος ονομάζονται Βυζαντινή Ανοχή Σφάλματος (BFT) μηχανισμοί συναίνεσης.

Ως Βυζαντινή Συναίνεση Ανεκτική σε Σφάλματα (Xiao et al. 2020) ορίζεται ένα πρωτόκολλο συναίνεσης ανεκτικό σε σφάλματα κατάρρευσης (CFT) ή Βυζαντινή Συναίνεση σε Σφάλματα (BFT) εάν μπορεί να ανεχθεί έναν ορισμένο αριθμό σφαλμάτων ή βλαβών βυζαντινής διεργασίας διατηρώντας παράλληλα την κανονική λειτουργία. Ο όρος «βυζαντινή» επινοήθηκε από τους Lamport et al. το 1982 όταν περιέγραφαν το Πρόβλημα των Βυζαντινών Στρατηγών, μια αλληγορική περίπτωση για τη συναίνεση μίας τιμής μεταξύ καταναμημένων διεργασιών. Η συνηθισμένη αιτία μιας αποτυχίας του Βυζαντίου είναι η εχθρική επίθεση, όπως η έγχυση κακόβουλου λογισμικού και η

κατάληψη φυσικής συσκευής. Πολλαπλές Βυζαντινές διεργασίες μπορεί να συνωμοτήσουν για να προκαλέσουν μεγαλύτερη ζημιά.

Λόγω της συμπεριληπτικής σχέσης που υπάρχει μεταξύ μιας βλάβης κατάρρευσης και μιας βυζαντινής βλάβης, ένα πρωτόκολλο συναίνεσης BFT είναι φυσικά CFT (σφάλματα κατάρρευσης). Η συναίνεση BFT ορίζεται από τις ακόλουθες τέσσερις απαιτήσεις:

- Τερματισμός: Κάθε μη ελαττωματική διεργασία αποφασίζει μια έξοδο.
- Συμφωνία: Κάθε μη ελαττωματική διεργασία τελικά αποφασίζει την ίδια έξοδο $\hat{y}$.
- Εγκυρότητα: Εάν κάθε διεργασία ξεκινά με την ίδια είσοδο $\hat{x}$, τότε $\hat{y} = \hat{x}$.
- Ακεραιότητα: Κάθε απόφαση μη ελαττωματικής διεργασίας και η τιμή συναίνεσης $\hat{y}$ πρέπει να έχουν προταθεί από κάποια μη ελαττωματική διεργασία.

Το TSBFT έχει ένα τυπικό ασύγχρονο μοντέλο συστήματος BFT και κοινές υποθέσεις ασφαλείας για το BFT. Από τους κόμβους στο σύστημα, ο επιτιθέμενος μπορεί να ελέγξει έως και f βυζαντινούς κόμβους και να επιτεθεί προσαρμοστικά σε αυτούς τους ελαττωματικούς κόμβους. Ένας επιτιθέμενος μπορεί να εμποδίσει ένα δίκτυο να επιτύχει συναίνεση διακόπτοντας την επικοινωνία μεταξύ των κόμβων. Αλλά έχουν περιορισμένη υπολογιστική ισχύ και δεν μπορούν να παραβιάσουν την ασφάλεια των αλγορίθμων κρυπτογράφησης (Tian and H. Xu, 2023)

5.7 Επίλυση συγκρούσεων

Λόγω της αιτιώδους εξάρτησης των διατεταγμένων συναλλαγών, οι συναλλαγές μπορούν να είναι συγκρουόμενες ακόμη και αν δεν καταναλώνουν την ίδια έξοδο. Δύο διακριτές συναλλαγές $x, y \in L$ είναι άμεσα συγκρουόμενες εάν έχουν τουλάχιστον μία κοινή είσοδο. Δύο συναλλαγές λέγονται συγκρουόμενες εάν είναι άμεσα ή έμμεσα συγκρουόμενες.

5.8 Σύγκριση μηχανισμών

Γενικά ένα ευρύ φάσμα πρωτοκόλλων συναίνεσης blockchain έχει προταθεί, συνοδευόμενο από αλγοριθμικές αφαιρέσεις και αναλύσεις τρωτότητας (Xiao et al. 2020).

1. Πρωτόκολλο DLS: Οι Dwork, Lynch, και Stockmeyer, πρότειναν επίσης ένα πρωτότυπο πρωτόκολλο συναίνεσης (DLS από τα ονόματα των συγγραφέων) που διαθέτει ένα πρωτόκολλο εκπομπής για κάθε κύκλο συναίνεσης. Το κρυπτονόμισμα Tendermint χρησιμοποιεί μια προσαρμοσμένη έκδοση του DLS για την οριστικοποίηση μπλοκ (Xiao et al. 2020).
2. Αναπαραγωγή με σήμανση Views (VR): Προτεινόμενη από τους Oki και Liskov το 1988, η αναπαραγωγή με σήμανση Views είναι ένα σχήμα αναπαραγωγής διακομιστή για την αντιμετώπιση σφαλμάτων διακομιστή. Αργότερα, επεκτάθηκε σε ένα πρωτόκολλο συναίνεσης από τους Liskov και Cowling το 2012, το οποίο αναφέρεται ως VR (Xiao et al. 2020).
3. Ανάκτηση. Ο κύριος διακομιστής λαμβάνει ένα αίτημα πελάτη και ξεκινά την κανονική λειτουργία. Σε περίπτωση σφάλματος του κύριου διακομιστή, το πρωτόκολλο αλλαγής προβολής ενεργοποιείται σε κάθε αντίγραφο ανά χρονικό όριο του μηνύματος "Προετοιμασία". Μεταδίδουν μηνύματα αλλαγής προβολής μεταξύ τους και μετρούν τις λήψεις. Αφού λάβει μηνύματα αλλαγής προβολής από περισσότερα από τα μισά αντίγραφα, το επόμενο στη σειρά αντίγραφο γίνεται το νέο κύριο και ενημερώνει τα άλλα να συνεχίσουν την κανονική λειτουργία. Το πρωτόκολλο ανάκτησης χρησιμοποιείται από οποιονδήποτε διακομιστή για την ανάκτηση από μια συντριβή. Η εικονική πραγματικότητα μπορεί να

ανεχθεί f αντίγραφα που έχουν υποστεί συντριβή εάν ο πληθυσμός του δικτύου $N \geq 2f + 1$. αλλά όχι βλάβες Byzantine (Xiao et al. 2020).

4. Paxos: Το Paxos είναι ένα σχήμα SMR που προτάθηκε από τον Lamport το 1989 και μιμείται το αρχαίο κοινοβούλιο μερικής απασχόλησης των Paxos και αργότερα επεξεργάστηκε το 2001. Σχεδιάστηκε ειδικά για συναίνεση ανεκτική σε σφάλματα, ενώ παράλληλα έχει πολλές ομοιότητες με την εικονική πραγματικότητα. Το Paxos ταξινομεί τους κόμβους σε τρεις ρόλους: προτείνοντες, αποδέκτες και μαθητές. Ένας προτείνων προτείνει μια τιμή στην αρχή και ο στόχος του συστήματος είναι να κάνει τους αποδέκτες να συμφωνήσουν σε μία μόνο τιμή και οι μαθητές να μάθουν αυτήν την τιμή από τους αποδέκτες. Στο σενάριο πελάτη-διακομιστή, ο πελάτης είναι ο μαθητής, ο κύριος είναι ο προτείνων και τα αντίγραφα είναι οι αποδέκτες. Μετά την ενημέρωση στην ίδια κατάσταση, όλοι οι διακομιστές εκτελούν το αίτημα και το στέλνουν στον πελάτη, ο οποίος στη συνέχεια επιλέγει το αποτέλεσμα της πλειοψηφίας. Όταν ο προτείνων υποστεί μια αποτυχία, οι αποδέκτες εκλέγουν έναν νέο ηγέτη μέσω μιας παρόμοιας διαδικασίας πρότασης-αποδοχής. Όπως και με το VR, το Paxos μπορεί να ανεχθεί f αποδέκτες που έχουν υποστεί συντριβή όταν $N \geq 2f + 1$, αλλά όχι βλάβες Byzantine. Ξεκινώντας από τον αρχικό του σχεδιασμό, το Paxos έχει εξελιχθεί σε μια οικογένεια πρωτοκόλλων συναίνεσης, συμπεριλαμβανομένων των multi-Paxos, των cheap Paxos και των fast-Paxos, καθένα από τα οποία έχει έναν συγκεκριμένο στόχο (Xiao et al. 2020).
5. Πρακτική Βυζαντινή Ανοχή Σφαλμάτων (PBFT): Το PBFT αναπτύχθηκε από τους Castro και Liskov το 1999, και είναι το πρώτο πρωτόκολλο συναίνεσης BFT που βασίζεται σε SMR και έχει κερδίσει ευρεία αναγνώριση λόγω της πρακτικότητας του. Έχει γίνει σχεδόν συνώνυμο με τη συναίνεση BFT στην κοινότητα blockchain. Το PBFT προήλθε από το πλαίσιο VR και εμπνεύστηκε από το Paxos. Το PBFT αποτελείται από τρία υποπρωτόκολλα: 1) Κανονική λειτουργία, 2) Σημείο ελέγχου και 3) Αλλαγή προβολής (Xiao et al. 2020).

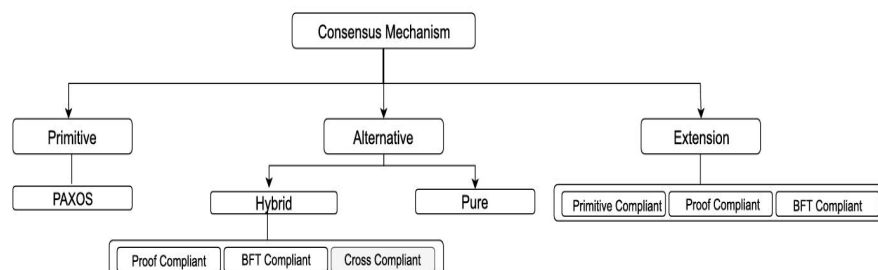
Το πρωτόκολλο Checkpoint χρησιμεύει ως εργαλείο καταγραφής που διατηρεί ένα συρόμενο παράθυρο (του οποίου το κατώτερο όριο είναι το σταθερό σημείο ελέγχου) για την παρακολούθηση των ενεργών αιτημάτων λειτουργίας. Το πιο πρόσφατο σταθερό σημείο ελέγχου χρησιμοποιείται για την ασφαλή απόρριψη παλαιότερων αιτημάτων στο αρχείο καταγραφής λειτουργίας και τη διευκόλυνση του πρωτοκόλλου αλλαγής προβολής. Σε περίπτωση αποτυχίας πρωτεύοντος, το πρωτόκολλο αλλαγής προβολής ενεργοποιείται σε κάθε αντίγραφο που ανιχνεύει το χρονικό όριο του μηνύματος του πρωτεύοντος. Απομακρύνουν τον υπάρχοντα πρωτεύοντα και μεταδίδουν μηνύματα αλλαγής προβολής μεταξύ τους και μετρούν τις λήψεις. Όσον αφορά την ανοχή σφαλμάτων, δεδομένου ότι ένας διακομιστής χρειάζεται να λάβει περισσότερα από $2f + 1$ μηνύματα Προετοιμασίας (Επικύρωσης) στη φάση Προετοιμασίας (Επικύρωσης) πριν προχωρήσει στην επόμενη ενέργεια, θα υπάρχουν τουλάχιστον $2f + 1$ (ως $N \geq 3f + 1$) έντιμοι διακομιστές στην ίδια κατάσταση μετά τη φάση Επικύρωσης και παράγοντας το ίδιο αποτέλεσμα. Οι f Βυζαντινοί διακομιστές δεν είναι σε θέση να επηρεάσουν τη συναίνεση της πλειοψηφίας. Επομένως, το PBFT μπορεί να ανεχθεί f Βυζαντινά αντίγραφα, όταν ο πληθυσμός των διακομιστών είναι $N \geq 3f + 1$, το οποίο είναι σε συμφωνία με το θεμελιώδες όριο $1/3$ BFT (Xiao et al. 2020).

Οι Wang et al. (2019) παρέχουν μια ολοκληρωμένη επισκόπηση των πρωτοκόλλων συναίνεσης blockchain και οι Wang et al. (2023) μια ανασκόπηση των συστημάτων που βασίζονται σε DAG, εξερευνώντας βασικές πτυχές όπως οι μηχανισμοί συναίνεσης, η ασφάλεια και η απόδοση. Παρουσιάζονται λεπτομερή σχήματα συναίνεσης, συμπεριλαμβανομένης της συναίνεσης Nakamoto, των σχημάτων συναίνεσης απόδειξης ιδέας και τεχνικών εικονικής εξόρυξης όπως η απόδειξη συμμετοχής (PoS) μαζί με την χρηστικότητα αξιόπιστου υλικού. Συζητείται επίσης ο υβριδισμός

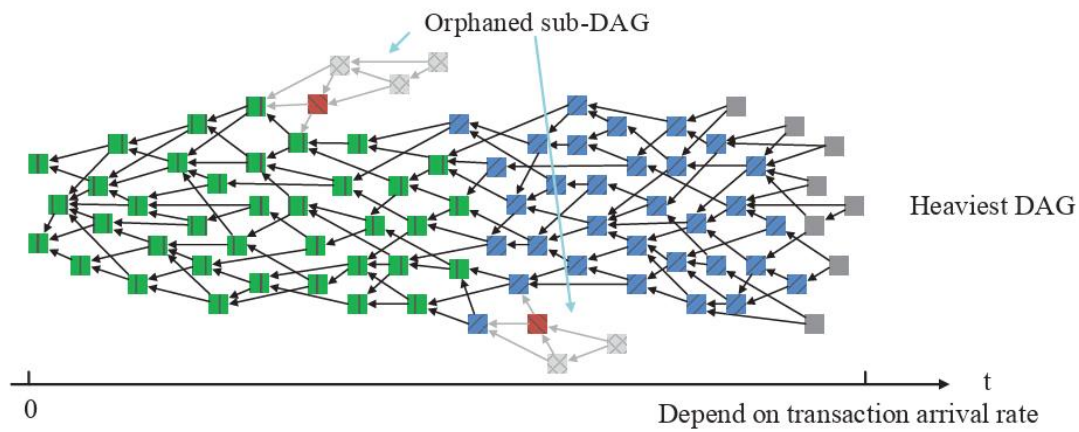
μεταξύ πρωτοκόλλων PoX και κλασικών BFT. Ο Vukolić, (2015) συγκρίνει δύο είδη πρωτοκόλλων συναίνεσης blockchain, τα πρωτόκολλα με βάση το PoW (Απόδειξη Εργασίας) και με βάση το BFT (Βυζαντινή Συναίνεση σε Σφάλματα), σε σχέση με την απόδοση συναλλαγών, τα όρια κλιμάκωσης, την οριστικότητα συναίνεσης και τις επιπτώσεις στην ασφάλεια. Τα πρωτόκολλα που βασίζονται στο PoW κλιμακώνονται με το μέγεθος του δικτύου και είναι κατάλληλα για blockchain χωρίς άδεια, αλλά αποδίδουν πολύ περιορισμένη απόδοση και μεγάλη καθυστέρηση επιβεβαίωσης. Συγκριτικά, τα πρωτόκολλα BFT έχουν ενσωματωμένη οριστικότητα συναίνεσης και επιτυγχάνουν πολύ υψηλότερη χωρητικότητα συναλλαγών, αλλά παρουσιάζουν υψηλή πολυπλοκότητα ανταλλαγής μηνυμάτων ανά μπλοκ και χρειάζονται ένα δίκτυο με άδεια για τη διαχείριση ταυτοτήτων. Ως αποτέλεσμα αυτού, δεν κλιμακώνονται καλά με το μέγεθος του δικτύου. Το TSBFT έχει ένα τυπικό ασύγχρονο μοντέλο συστήματος BFT και κοινές υποθέσεις ασφαλείας για το BFT. Από τους κόμβους στο σύστημα, ο επιτιθέμενος μπορεί να ελέγξει έως και f βυζαντινούς κόμβους και να επιτεθεί προσαρμοστικά σε αυτούς τους ελαττωματικούς κόμβους. Ένας επιτιθέμενος μπορεί να εμποδίσει ένα δίκτυο να επιτύχει συναίνεση διακόπτοντας την επικοινωνία μεταξύ των κόμβων. Αλλά έχουν περιορισμένη υπολογιστική ισχύ και δεν μπορούν να παραβιάσουν την ασφάλεια των αλγορίθμων κρυπτογράφησης (Tian et al 2023).

Μια οικογένεια πρωτοκόλλων συναίνεσης, που ονομάζεται Snow consensus, αντιμετωπίζει τους περιορισμούς των υπάρχουσών μεθόδων συναίνεσης, όπως αυτές που χρησιμοποιούν απόδειξη εργασίας ή απαρτίες. Οι αλγόριθμοι συναίνεσης Snow βασίζονται σε μια φυσική, τυχαιοποιημένη ρουτίνα, όπου οι συμμετέχοντες λαμβάνουν συνεχώς δείγματα υποσυνόλων άλλων και υιοθετούν μια παρατηρούμενη πλειοψηφική τιμή μέχρι να επιτευχθεί συναίνεση. Επιπλέον, η Snow consensus ορίζει συνθήκες με βάση τις τοπικές απόψεις και τις παραμέτρους ασφαλείας των συμμετεχόντων. Τα πρωτόκολλα Snow αποτελούν τη βάση για τα blockchains τύπου Avalanche (Cachin 2014)

Στο IOTA Tangle, κάθε συναλλαγή χρησιμεύει ως η μικρότερη μονάδα συναίνεσης, με τη μέθοδο MarkovChain MonteCarlo (MCMC) που χρησιμοποιείται για την προσάρτηση νέων συναλλαγών και τη διατήρηση μιας ισορροπίας κατανομής εντός του δικτύου. Η συναίνεση επιτυγχάνεται μέσω της επικύρωσης συναλλαγών που εκτελείται από όλους τους κόμβους, η οποία διασφαλίζει την αποκέντρωση, την ασφάλεια και την ευρωστία, χωρίς την ανάγκη ενός παραδοσιακού συστήματος Proof-of-Work (PoW) για την εξόρυξη. Αντ' αυτού, το IOTA χρησιμοποιεί έναν ελαφρύ μηχανισμό PoW αποκλειστικά για την αποτροπή ανεπιθύμητων μηνυμάτων και ανέντιμων συναλλαγών (Ramírez-Gordillo 2025).



Εικόνα 5.2 Ταξινόμηση μηχανισμών συναίνεσης Πηγή : Lashkari and Musilek (2021)



Εικόνα 5.3 Η μεγαλύτερη αλυσίδα σε PoW έναντι του βαρύτερου DAG στο Tangle

Πίνακας 5.1 Σύγκριση μηχανισμών συναίνεσης

Μηχανισμός	Πλεονεκτήματα	Μειονεκτήματα
Nakamoto Consensus		
PoW	Υψηλή ασφάλεια	Μεγάλη κατανάλωση ενέργειας
PoS	Χαμηλή κατανάλωση ενέργειας	Συγκέντρωση ισχύος
BFT	Γρήγορη οριστικοποίηση	Περιορισμένη κλιμάκωση
DAG Consensus	Υψηλή επεκτασιμότητα	Σχετικά νέα

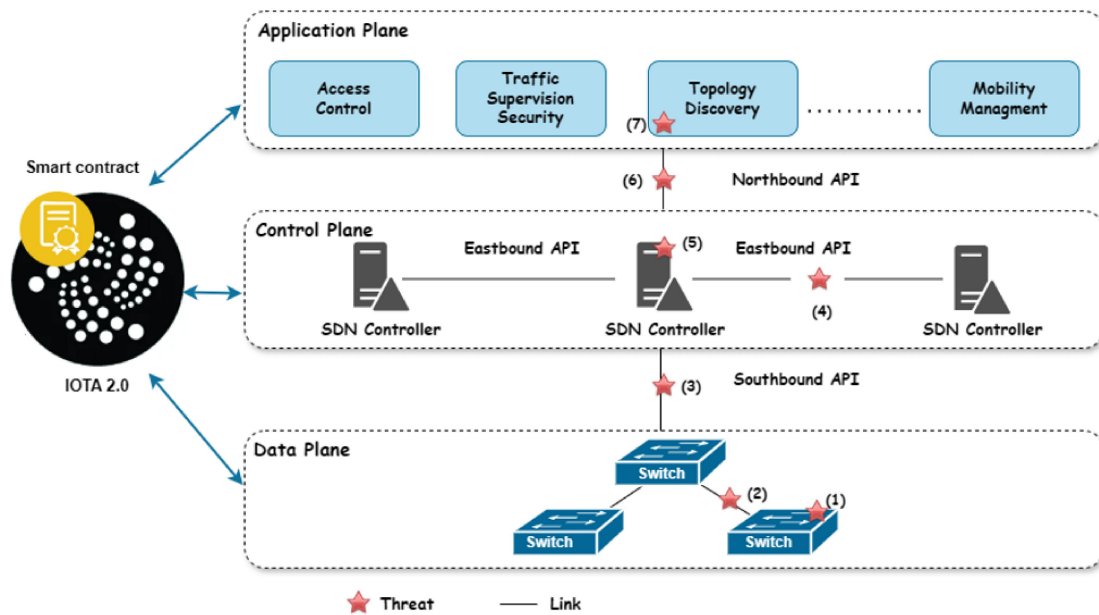
Κεφάλαιο 6ο: Προκλήσεις (ασφάλεια, επεκτασιμότητα, ιδιωτικότητα)

6.1 Ασφάλεια

Ο ταχέως αναπτυσσόμενος τομέας του Διαδικτύου των Πραγμάτων (IoT), και η ευρεία υιοθέτηση αυτών των τεχνολογιών αντιμετωπίζει σημαντικές προκλήσεις, στη διαχείριση ταυτοτήτων, το απόρρητο των δεδομένων και ιδιαίτερα ζητήματα ασφάλειας, επειδή η διαμόρφωση των υποδομών και οι πολιτικές ασφάλειας που χρησιμοποιούνται σε αυτόν τον νεοσύστατο τομέα δεν έχουν ακόμη ωριμάσει (Al Mamun 2021). Τα συμβατικά συστήματα διαχείρισης ταυτοτήτων λειτουργούν κυρίως μέσω ενός κεντρικού πλαισίου, εξαρτώμενα από μια ενιαία αρχή για την επαλήθευση και τη διαχείριση των ταυτοτήτων των συσκευών. Παρόλο που αυτά τα συστήματα λειτουργούν επαρκώς σε συγκεκριμένες περιπτώσεις, έχουν εγγενώς ευπάθειες, όπως μοναδικά σημεία αποτυχίας, περιορισμένη επεκτασιμότητα και περιορισμένο απόρρητο δεδομένων. Αυτά τα ζητήματα γίνονται πιο έντονα σε εφαρμογές IoT μεγάλης κλίμακας, όπου ο αριθμός των διασυνδεδεμένων συσκευών μπορεί να επιβαρύνει τις κεντρικές δομές, αυξάνοντας έτσι τις πιθανότητες παραβιάσεων ασφαλείας και διακοπών του συστήματος (Ramírez-Gordillo 2025). Για την αντιμετώπιση αυτού του ζητήματος, έχουν προταθεί και προωθηθεί πολλές βελτιστοποιημένες δομές, που καλύπτουν τόσο τις δομές δεδομένων όσο και τις τοπολογίες. Αυτές οι δομές έχουν βελτιστοποιηθεί για διαφορετικά υπόβαθρα υλοποίησης, π.χ., χρησιμοποιώντας blockchain για τη βελτίωση της ασφάλειας των δεδομένων.

Η ακεραιότητα των δεδομένων και η προστασία της ασφάλειας είναι απαραίτητες στο Διαδίκτυο των Πραγμάτων. Η τεχνολογία Blockchain αναπτύσσεται με βάση τη φιλοσοφία σχεδιασμού για την ασφάλη, διαφανή και αποκεντρωμένη εκτέλεση και αποθήκευση συναλλαγών. Η τεχνολογία IOTA με δομή Directed Acyclic Graph (DAG) αποτελεί μια λύση για την πραγματοποίηση ασφαλών και κλιμακώσιμων συναλλαγών δεδομένων.

Τέτοια συστήματα έχουν δύο κύριες πρόσθετες απαιτήσεις σήμερα (i) την ανάγκη για απόδοση (σχεδόν) σε πραγματικό χρόνο για να εξυπηρετήσουν τη λειτουργία τους, αποφεύγοντας την ανάλυση δεδομένων εκτός σύνδεσης και (ii) ασφάλεια από άκρο σε άκρο με έλεγχο ταυτότητας πηγής δεδομένων, εμπιστευτικότητα και ακεραιότητα δεδομένων από τον αισθητήρα σε απομακρυσμένη τοποθεσία όπου αποθηκεύονται και υποβάλλονται σε επεξεργασία τα δεδομένα. Τα ζητήματα ασφάλειας από άκρο σε άκρο είναι ύψιστης σημασίας και συχνά καθοδηγούν την επιλογή της λύσης. Η κοινή μέθοδος προστασίας της μετάδοσης δεδομένων σε συστήματα αισθητήρων είναι η Ασφάλεια Επιπέδου Μεταφοράς (TLS) ή το αντίστοιχο datagram της, η Ασφάλεια Επιπέδου Μεταφοράς Datagram (DTLS). Το (D)TLS είναι ένα απίστευτα ισχυρό και ευέλικτο ασφαλές πρωτόκολλο για τη δημιουργία ασφαλών καναλιών επικοινωνίας μεταξύ συσκευών (Carelli et al. 2022).



Εικόνα 6.1 Ανάλυση απειλών ασφαλείας και ευπαθειών στο SDN ανά επίπεδο. Πηγή: Fartitchou et al (2024)

6.2 Επιθέσεις

Το IOTA σύμφωνα με έρευνες, εξακολουθεί να αντιμετωπίζει το ζήτημα της ευπάθειας σε επιθέσεις διαχωρισμού και συναλλαγές που δεν έχουν απομείνει. Η επίθεση διαχωρισμού προκαλεί την επιβεβαίωση συναλλαγών σύγκρουσης από το δίκτυο. Στη συνέχεια, οι συναλλαγές που δεν έχουν απομείνει προκαλούν τη δημιουργία συναλλαγών που δεν θα επιβεβαιωθούν από το δίκτυο. Ο αλγόριθμος τυχαίας περιπλάνησης με βάση την άκρη επιλογής (WRW) χρησιμοποιεί την αλυσίδα Markov Monte Carlo (MCMC) για να ξεπεράσει αυτά τα δύο ζητήματα εφαρμόζοντας την κατάλληλη παράμετρο πόλωσης (α). Ωστόσο, όταν η παράμετρος πόλωσης (α) είναι πολύ μεγάλη, θα παράξει πολλές συναλλαγές που δεν έχουν απομείνει. Ο προσδιορισμός της βέλτιστης τιμής του α εξακολουθεί να αποτελεί αντικείμενο για έρευνα (Rochman et al. 2023).

Επιθέσεις που βασίζονται σε δωροδοκία Κατά τη διάρκεια μιας επίθεσης δωροδοκίας, ένας εισβολέας προσπαθεί να δημιουργήσει ένα νέο κύριο κλάδο δίνοντας κίνητρα στους κόμβους να επικυρώσουν να εργαστούν σε μια συγκεκριμένη διακλάδωση του σχεδιασμού DLT, την οποία ο εισβολέας ελέγχει. Έτσι, ο αριθμός των κόμβων που εργάζονται στον κλάδο του εισβολέα αυξάνεται και ο κλάδος του εισβολέα μπορεί τελικά να προλάβει τον κύριο κλάδο του blockchain και, τέλος, να γίνει ο κύριος κλάδος (Kannengießer et al. 2019).

Επιθέσεις που βασίζονται σε κατατμήσεις. Οι επιθέσεις που βασίζονται σε κατατμήσεις μπορούν να εκτελεστούν με επιτυχία σε σχέδια DLT χωρίς δημόσια άδεια με πιθανοτική οριστικότητα (π.χ., Bitcoin και Ethereum). Σε τέτοια σχέδια DLT, μπορούν να αξιοποιηθούν διακλαδώσεις (fork) για την εκτέλεση επιθέσεων στην ακεραιότητα του κατανεμημένου καθολικού. Οι πιο δημοφιλείς επιθέσεις είναι οι επιθέσεις 51%, οι επιθέσεις ισορροπίας (balance) και οι επιθέσεις έκλειψης (eclipse). Μια επίθεση 51% μπορεί να είναι επιτυχής σε σχέδια DLT με μηχανισμό συναίνεσης (consensus mechanism) που βασίζεται σε μια απόφαση πλειοψηφίας μεταξύ των κόμβων (π.χ., Nakamoto Consensus) (Kannengießer et al., 2019).

Επιθέσεις εγωιστικής εξόρυξης Οι επιθέσεις εγωιστικής εξόρυξης περιγράφουν ένα φαινόμενο όπου ένα σύνολο κόμβων εργάζεται στον δικό του κλάδο ενός blockchain χωρίς να δημοσιεύει τα μπλοκ του στον κύριο κλάδο μέχρι να επιλεγεί ο κλάδος τους ως μελλοντικός κύριος κλάδος από τον κανόνα επίλυσης fork που εφαρμόζεται στο κατανεμημένο καθολικό. Μια επίθεση εγωιστικής εξόρυξης πραγματοποιείται από τους εισβολείς για να λάβουν υπερβολικές ανταμοιβές ή να σπαταλήσουν την υπολογιστική ισχύ των ειλικρινών κόμβων επικύρωσης. Για να πραγματοποιηθεί μια επιτυχημένη επίθεση εγωιστικής εξόρυξης σε Bitcoin πρέπει να συνεργεί τουλάχιστον το ένα τρίτο των κόμβων επικύρωσης (Kannengießer et al 2019).

Επίθεση μεγάλης εμβέλειας. Μια επίθεση μεγάλης εμβέλειας στοχεύει να ξαναγράψει το ιστορικό συναλλαγών από το μπλοκ γένεσης (το πρώτο μπλοκ σε ένα blockchain). Μια επίθεση μεγάλης εμβέλειας είναι επιτυχημένη όταν ο εισβολέας έχει δημιουργήσει ένα fork, το οποίο έχει γίνει η κύρια αλυσίδα, κάτι που είναι παρόμοιο με την εγωιστική εξόρυξη (ή επίθεση μικρής εμβέλειας). Επιρρεπή σε επιθέσεις μεγάλης εμβέλειας είναι κυρίως τα σχέδια DLT, τα οποία βασίζονται στην Απόδειξη Συμμετοχής ως μηχανισμό συναίνεσης, ενώ οι επιθέσεις μεγάλης εμβέλειας θεωρούνται μη πρακτικές για σχέδια DLT που βασίζονται σε PoW, επειδή τα σχέδια DLT που βασίζονται σε PoW απαιτούν υπερβολική υπολογιστική προσπάθεια για να ξαναγράψουν το ιστορικό συναλλαγών ξεκινώντας από το μπλοκ γένεσης (Kannengießer et al 2019)..

Ανωμαλία Blockchain. Η ανωμαλία blockchain αναφέρεται στο γεγονός ότι ένα blockchain δεν μπορεί να εγγραφεί ότι μια συνδεδεμένη συναλλαγή περιλαμβάνεται μόνιμα σε μια διακλάδωση ενός blockchain. Λόγω αυτού, οι υπό όρους συναλλαγές είναι δύσκολο να εκτελεστούν. Η ανωμαλία του blockchain μπορεί να συμβεί σε blockchains των οποίων ο μηχανισμός συναίνεσης δεν διασφαλίζει ντετερμινιστική συμφωνία μεταξύ κόμβων και ασφάλεια συναίνεσης (Kannengießer et al 2019).

Συμπλική Επίθεση. Σε μια επίθεση sibyl, ο εισβολέας δημιουργεί πολλαπλούς (εικονικούς) κόμβους για να συμβάλει η πλειοψηφία των παραγόντων στην εύρεση συναίνεσης και τελικά να ξαναγράψει το ιστορικό συναλλαγών του κατανεμημένου καθολικού. Για να μειωθεί η πιθανότητα επιτυχημένων επιθέσεων sibyl, όλοι οι κόμβοι πρέπει να εκτελέσουν ένα συγκεκριμένο PoW, όπου κάθε κόμβος πρέπει πρώτα να ολοκληρώσει μια υπολογιστικά δύσκολη εργασία, η οποία μπορεί εύκολα να αξιολογηθεί από άλλους κόμβους (Kannengießer et al 2019).

6.3 Επεκτασιμότητα

Τα τελευταία χρόνια, εργασίες των Gueta, et al., 2019, Liu, et al. (2019) και Yin, et al (2019) έχουν ξεπεράσει τους περιορισμούς απόδοσης και επεκτασιμότητας του πρωτοκόλλου BFT για να παρέχουν εύλογη ασφάλεια και ζωντάνια. Ωστόσο, παραμένουν οι ακόλουθες τρεις προκλήσεις: (1) Αποτυχία ενός σημείου. Στην περίπτωση του πρωτοκόλλου BFT που βασίζεται σε ηγέτη, εάν οι αντίπαλοι εξαπολύσουν μια επίθεση DDOS στον ηγέτη, το πρωτόκολλο ενδέχεται να μην λειτουργήσει σωστά. (2) Τεράστιος συνολικός όγκος μηνυμάτων. Σε πολλά συστήματα blockchain, οι συναλλαγές συχνά ομαδοποιούνται για επεξεργασία σε μεγάλα μπλοκ, για να μειωθεί το κόστος συναίνεσης. Ωστόσο, επειδή το μπλοκ συνήθως μεταδίδεται με μοτίβο ένα προς όλα, ή όλα προς όλα, αυτό προκαλεί μια σημαντική αύξηση του συνολικού όγκου μηνυμάτων στη διαδικασία μετάδοσης. (3) Η αποτελεσματικότητα της συναίνεσης περιορίζεται από έναν μόνο πιο αργό κόμβο. Τα επικοινωνιακά και υπολογιστικά κόστη σε έναν μόνο κόμβο περιορίζουν την επεκτασιμότητα του πρωτοκόλλου. Διαφορετικοί κόμβοι έχουν διαφορετικές ικανότητες λήψης και επεξεργασίας μηνυμάτων από άλλους κόμβους, με αποτέλεσμα οι άλλοι κόμβοι να περιμένουν τον πιο αργό κόμβο (Tian and Xu 2023). Οι υπάρχουσες λύσεις είτε δεν αντιμετωπίζουν αυτές τις προκλήσεις, είτε δεν υπάρχει ισορροπία μεταξύ ασφάλειας και απόδοσης. Συγκεκριμένα, το PBFT (Πρακτική Βυζαντινή Ανοχή Σφαλμάτων) και οι

παραλλαγές του διασφαλίζουν ότι ο ηγέτης είναι ιδιαίτερα διαθέσιμος, ενεργοποιώντας ακριβή πρωτόκολλα για να αντικαταστήσουν τον ηγέτη μόλις χάσει τη δραστηριότητά του. Όλοι οι συμμετέχοντες γνωρίζουν εκ των προτέρων για τον επόμενο ηγέτη πριν ξεκινήσουν επιθέσεις, αποτυγχάνοντας έτσι να λύσουν τις προκλήσεις 1 και 3, που περιγράφηκαν παραπάνω. Άλλες λύσεις χρησιμοποιούν ψηφιακές υπογραφές για να αντιμετωπίσουν την πρόκληση 2, όπως το FBFT και το Hotstuff, τα οποία χρησιμοποιούν τεχνολογία υπογραφής κατωφλίου BLS για τη συμπίεση μηνυμάτων και τη μείωση του συνολικού όγκου μηνυμάτων. Άλλα σχήματα, όπως το Algorand, επιλέγουν τυχαία μέλη της επιτροπής μέσω κρυπτογραφικής κλήρωσης και σε συνδυασμό με το πρωτόκολλο Byzantine Agreement (BA) για την επίτευξη συναίνεσης. Αυτό το πρωτόκολλο μπορεί να αποφύγει αποτελεσματικά τις προσαρμοστικές επιθέσεις, αλλά θα παράγει μια τεράστια ποσότητα δεδομένων υπογραφής κατά τη διάρκεια της διαδικασίας συναίνεσης, με αποτέλεσμα την απώλεια αποθήκευσης και την αδυναμία να αντιμετωπιστούν οι προκλήσεις 1 και 2, ενώ αντιμετωπίζει την πρόκληση 3 (Tian and Xu 2023).

6.4 Ιδιωτικότητα

Τα περισσότερα DLT που βασίζονται σε DAG έχουν μη κρυπτογραφημένα μεταδεδομένα απλού κειμένου στα καθολικά τους βιβλία και υποστηρίζουν διευθύνσεις με ψευδώνυμο. Αυτό καθιστά τα DLT που βασίζονται σε DAG μια μη ελκυστική λύση στην περίπτωση που οι εφαρμογές απαιτούν προστασία απορρήτου. Λόγω των δεδομένων απλού κειμένου στο καθολικό αυτών των DLT, ένας κακόβουλος μπορεί να παρακολουθήσει τους σχετικούς λογαριασμούς χρησιμοποιώντας εργαλεία ανάλυσης δεδομένων, παρεμποδίζοντας την ταυτότητα των χρηστών και στη συνέχεια διεξάγοντας επιβλαβείς δραστηριότητες έτσι ώστε να κλέψει ή να παγώσει τα κεφάλαιά τους. Με αυτόν τον τρόπο, το απόρρητο των ταυτοτήτων των χρηστών, τα δεδομένα συναλλαγών και η συνδεσιμότητα μεταξύ των συναλλαγών τίθενται σε κίνδυνο. Στον τομέα του blockchain, αυτά τα ζητήματα έχουν αντιμετωπιστεί με τη χρήση τεχνικών διατήρησης της ιδιωτικότητας ή με τη δημιουργία συστημάτων blockchain με επίκεντρο την ιδιωτικότητα (Raikwar 2025).

Η ιδιωτικότητα στα κατανεμημένα καθολικά αφορά τόσο την ιδιωτικότητα ταυτότητας όσο και την ιδιωτικότητα δεδομένων, συμπεριλαμβανομένων των ποσών των συναλλαγών και των υπολοίπων χρηστών. Έννοιες όπως η μη σύνδεση και η μη ιχνηλασιμότητα των συναλλαγών συμβάλλουν επίσης στη συζήτηση περί ιδιωτικότητας. Διάφορα συστήματα κρυπτονομισμάτων τα οποία βασίζονται στην τεχνολογία blockchain, που επικεντρώνονται στην ιδιωτικότητα, δίνουν προτεραιότητα στην εμπιστευτικότητα των χρηστών και των δεδομένων, και για να διασφαλίσουν την ιδιωτικότητα χρησιμοποιούν διάφορες κρυπτογραφικές τεχνικές. Ωστόσο, τα υπάρχοντα DLT που βασίζονται σε DAG, δίνουν προτεραιότητα κυρίως στη βελτίωση της απόδοσης, παραμερίζοντας την ιδιωτικότητα των χρηστών και των συναλλαγών, για να αποφευχθεί η πολυπλοκότητα που μπορεί να επηρεάσει τους χρόνους επιβεβαίωσης των συναλλαγών (Raikwar 2025). Ωστόσο, καθώς οι κρυπτογραφικές μέθοδοι ωριμάζουν, τεχνικές όπως οι αποδείξεις μηδενικής γνώσης, οι υπογραφές δακτυλίου και τα ανώνυμα κανάλια μετάδοσης για την ιδιωτικότητα ταυτότητας ή την ανάμειξη συναλλαγών, οι εμπιστευτικές συναλλαγές και η κρυπτογράφηση για την ιδιωτικότητα δεδομένων σε DLT που βασίζονται σε DAG, θα μπορούσαν να αποδειχθούν πλεονεκτικές. Τεχνικές όπως η ομοιορφική κρυπτογράφηση, τα σχήματα δέσμευσης, ο υπολογισμός πολλαπλών μερών και η διαφορική προστασία απορρήτου θα μπορούσαν να ενισχύσουν περαιτέρω την ιδιωτικότητα σε αυτά τα συστήματα (Raikwar 2025).

Προκειμένου να διασφαλιστεί η ιδιωτικότητα, το IOTA ανέπτυξε ένα πρωτόκολλο που ονομάζεται Masked Authenticating Messaging (MAM). Στο πλέγμα, κάθε συναλλαγή φέρει ένα μήνυμα, το οποίο επιτρέπει την ανταλλαγή αυτών των μηνυμάτων μεταξύ των κόμβων. Αυτό υποδεικνύει ότι

οποιοσδήποτε μπορεί να δει τα μηνύματα στο δίκτυο. Το MAM χρησιμοποιεί το σχήμα υπογραφής που βασίζεται στο Merkle tree και επιτρέπει την προστασία της ιδιωτικής ζωής κρυπτογραφώντας δεδομένα. Η κρυπτογράφηση πραγματοποιείται μέσω τριών τεχνικών, όπως είναι η ιδιωτική λειτουργία, η δημόσια λειτουργία και η περιορισμένη λειτουργία, επιτρέποντας έτσι την προστασία της ιδιωτικής ζωής (Alsbouei et al. 2019).

6.5 Διπλές δαπάνες- αντικρουόμενες συναλλαγές

Μια συναλλαγή περιλαμβάνει επίσης τη λύση «σε ένα παζλ απόδειξης εργασίας» και εγκρίνει δύο ή οποιοσδήποτε $k \geq 2$ συναλλαγές συμπεριλαμβάνοντας ένα hash από αυτές στη συναλλαγή. Αυτό δημιουργεί το DAG, με μια ακμή που δείχνει από κάθε επιβεβαιωμένη συναλλαγή προς τη νέα. Ένα βάρος (υπολογιστική εργασία) αποδίδεται στη συναλλαγή αναλογικά με τη δυσκολία του παζλ που ο κόμβος έχει «λύσει για την παραγωγή του». Ο κόμβος υποτίθεται ότι επιλέγει τις k συναλλαγές για να επιβεβαιώσει τυχαία, από όλες τις «συναλλαγές που γνωρίζει», και για να επαληθεύσει τις δύο συναλλαγές συν όλες τις μεταβατικές προηγούμενες συναλλαγές αυτών. Έμμεσα, θα πρέπει επίσης να επαληθεύει τη/τις συναλλαγή/ές που έχουν προηγούμενως αντιστοιχίσει τα διακριτικά στον/στους κόμβο. Η άνοδος μπορεί να εξαπατήσει 1) εκδίδοντας μια άκυρη συναλλαγή (διπλή δαπάνη), ή 2) συμπεριλαμβάνοντας άκυρες προ-προηγούμενες συναλλαγές ή τέλος 3) μη επιλέγοντας τις συναλλαγές για τυχαία επιβεβαίωση. Ωστόσο, άλλοι κόμβοι διαισθητικά δεν θα συμπεριλάμβαναν άκυρες συναλλαγές που παράγονται από το (1) ή το (2) και επομένως μια τέτοια συναλλαγή θα έμεινε ορφανή. Σε ένα πυκνό γράφημα, αναμένεται ότι οι περισσότερες συναλλαγές μιας συγκεκριμένης ηλικίας εγκρίνονται από τη συντριπτική πλειοψηφία όλων των νεοδημιουργημένων συναλλαγών. Το πόσο έντονα μια νέα συναλλαγή εγκρίνει τις προηγούμενες συναλλαγές της εξαρτάται από το βάρος, δηλαδή, την υπολογιστική εργασία, που απαιτήθηκε για την παραγωγή της. Η σταθερότητα του συστήματος βασίζεται στην υπόθεση ότι η πλειοψηφία της υπολογιστικής ισχύος μεταξύ των κόμβων συμπεριφέρεται σωστά (Cachin και Vukolic' 2017).

Σε επιθέσεις που βασίζονται σε κατατμήσεις, εάν οι επιτιθέμενοι ελέγχουν την πλειονότητα των κόμβων, μπορούν να ξαναγράψουν το ιστορικό συναλλαγών επειδή η πλειοψηφία των κόμβων τους συμφωνεί με την επιθυμητή (δόλια) κατάσταση του κατανεμημένου καθολικού. Σε σχέδια DLT όπως το Bitcoin, όπου οι κόμβοι μπορούν να ενταχθούν και να αποχωρήσουν αυθαίρετα από το δίκτυο, απαιτούνται μηχανισμοί για να αποτρέψουν τους επιτιθέμενους από το να δημιουργήσουν έναν τεράστιο αριθμό εικονικών κόμβων. Τέτοιοι μηχανισμοί συνήθως χρησιμοποιούν απόδειξη εργασίας, όπου οι κόμβοι πρέπει πρώτα να κάνουν υπολογιστική εργασία πριν μπορέσουν να καταχωρηθούν νέα δεδομένα στο κατανεμημένο καθολικό. Μια επίθεση ισορροπίας ενσωματώνει τη διαδικασία παροδικής διακοπής των επικοινωνιών μεταξύ υποομάδων κόμβων επικύρωσης με ίση υπολογιστική ισχύ, η οποία καθορίζεται, για παράδειγμα, από τον ρυθμό κατακερματισμού των κόμβων. Ενώ η επικοινωνία διακόπτεται, οι συναλλαγές μπορούν να υποβληθούν σε μια υποομάδα ενώ ο εισβολέας εξορύσσει σε μια άλλη υποομάδα. Στόχος των εισβολέων είναι να υπερισχύσουν του κλάδου blockchain στον οποίο υπέβαλαν συναλλαγές με τον κλάδο blockchain στον οποίο εργάζονται για να αυξήσουν την πιθανότητα επιτυχούς διπλής δαπάνης. Ως αποτέλεσμα, το ημερολόγιο μπορεί να ξαναγραφεί οποιαδήποτε στιγμή προτιμά ο εισβολέας.

Σε μια επίθεση έκλειψης, οι εισβολείς στοχεύουν σε τμήματα δικτύου καθυστερώντας ή εμποδίζοντας την προώθηση μηνυμάτων (π.χ., συναλλαγές) σε κόμβους του τμήματος δικτύου που δέχτηκε την επίθεση. Λόγω της καθυστέρησης των μηνυμάτων, οι στοχευμένοι κόμβοι απομονώνονται από το δίκτυο. Τέτοια τμήματα δικτύου διευκολύνουν τη διπλή δαπάνη. Για παράδειγμα, ένας επιτιθέμενος κόμβος θα έστελνε μια συναλλαγή (π.χ., μια πληρωμή) στον κόμβο-θύμα. Ο κόμβος-θύμα επικυρώνει τη συναλλαγή και, στη συνέχεια, επισκιάζεται από το δίκτυο από τον εισβολέα. Στη συνέχεια, ο

εισβολέας εκδίδει μια άλλη συναλλαγή σε ολόκληρο το δίκτυο και ξοδεύει ξανά τα ίδια περιουσιακά στοιχεία. Δεδομένου ότι όλες οι επιθέσεις που βασίζονται σε διαμερίσματα στοχεύουν στην ασυμμετρία πληροφοριών μεταξύ των κόμβων, οι επιθέσεις που βασίζονται σε διαμερίσματα μπορούν να εκτελεστούν με επιτυχία σε συνδυασμό με επιθέσεις δρομολόγησης (δηλαδή, επίθεση hijacking πρωτοκόλλου Border Gateway). Στις επιθέσεις δρομολόγησης, οι εισβολείς χειραγωγούν κόμβους ή φορείς εκμετάλλευσης δικτύου για να καθυστερήσουν σκόπιμα τα μηνύματα δικτύου.

Στην περίπτωση επιθέσεων επίθεση sybil, π.χ. στο Bitcoin, το Ethereum και το Nano, ο εκδότης του μπλοκ (ή της συναλλαγής) πρέπει πρώτα να μαντέψει μια nonce με μια αντίστοιχη τιμή hash, η οποία πληροί μια εύκολη στην επικύρωση συνθήκη (π.χ., ξεκινώντας με έναν καθορισμένο ελάχιστο αριθμό μηδενικών). Οι επιθέσεις Sybil μπορούν να εκτελεστούν για να απομονώσουν (ειλικρινείς) κόμβους από το δίκτυο μη αναμεταδίδοντας συναλλαγές αυτών των κόμβων. Η επιλεκτική αναμετάδοση συναλλαγών μπορεί να συμβάλει σε διπλές δαπάνες (Kannengießer et al 2019).

6.6 Διαλειτουργικότητα

Η πλήρης ανάπτυξη συστημάτων DLT και ψηφιακών πλατφορμών εξακολουθεί να είναι περιορισμένη, καθώς ορισμένα συστήματα λειτουργούν μεμονωμένα. Επομένως, η διαλειτουργικότητα του DLT είναι μία από τις προκλήσεις που εμποδίζουν την ευρεία υιοθέτηση των πλατφορμών DLT. Η διαλειτουργικότητα του DLT αντιπροσωπεύει την ικανότητα μιας καταναεμημένης πλατφόρμας καθολικού να αλληλεπιδρά και να μοιράζεται δεδομένα με άλλες παλαιές ψηφιακές εφαρμογές. Είναι αναπόφευκτο να ενορχηστρωθούν αυτά τα τμήματα ψηφιακών πλατφορμών εισάγοντας μια ενοποίηση πλατφόρμας μεταξύ DLT για τη διαχείριση της χρήσης δεδομένων εντός του ΕΕ. Προς το παρόν, οι ήδη προτεινόμενες προσεγγίσεις για τη διαλειτουργικότητα του DLT, όπως η αφελής αναμετάδοση, η πλευρική αλυσίδα, το σχήμα συμβολαιογραφικού ελέγχου λύσεων oracle ή η αλυσίδα αναμετάδοσης, δεν χρησιμοποιούνται ως επί το πλείστον, καθώς είτε απαιτούν πολλούς πόρους είτε είναι πολύ ακριβές για λειτουργία.

Μια επιπλέον πρόκληση είναι η αποτυχία διεργασίας. Μια διεργασία υφίσταται σφάλμα εάν σταματά απότομα να λειτουργεί χωρίς να συνεχίσει. Οι συνήθεις αιτίες ενός τέτοιου σφάλματος μπορεί να είναι η διακοπή ρεύματος, τα σφάλματα λογισμικού και οι επιθέσεις DoS. Μια βυζαντινή αποτυχία, ωστόσο, είναι πολύ πιο σοβαρή, καθώς η διεργασία μπορεί να ενεργήσει αυθαίρετα ενώ φαίνεται κανονική. Μπορεί να στείλει αντιφατικά μηνύματα σε άλλες διεργασίες με την ελπίδα να σαμποτάρει τη συναίνεση.

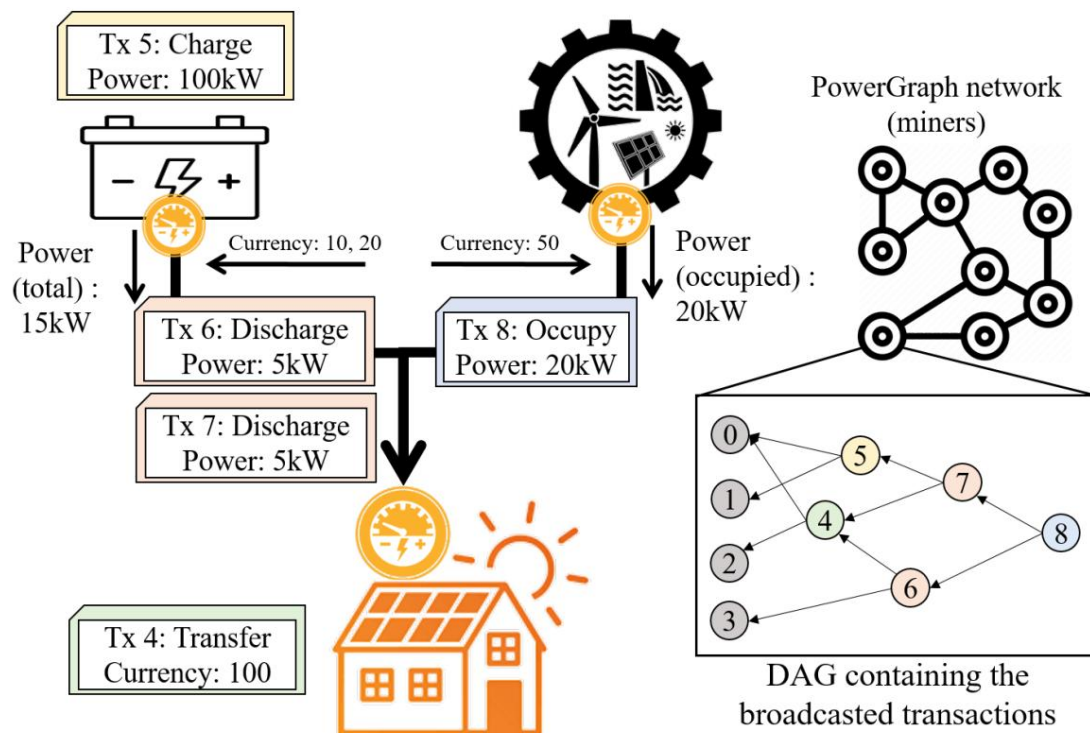
Οι προκλήσεις στα πρωτόκολλα συναίνεσης που βασίζονται σε DAG σε σύγκριση με τις αλυσίδες μπλοκ σύμφωνα με τους Raikwar et al. (2025) είναι οι ακόλουθες:

- 1) Κίνδυνοι ασφαλείας: Η αυξημένη πολυπλοκότητα των δομών DAG εισάγει πρόσθετους πιθανούς φορείς επίθεσης, καθώς τα πιο περίπλοκα συστήματα συχνά έχουν ένα ευρύτερο φάσμα τρωτών σημείων, σε σύγκριση με τα απλούστερα πρωτόκολλα.
- 2) Κατανόηση και υιοθέτηση: Τα πρωτόκολλα συναίνεσης που βασίζονται σε DAG δεν γίνονται εύκολα κατανοητά και δύσκολα υιοθετούνται, λόγω της πιο σύνθετης φύσης αυτών των πρωτοκόλλων, ιδιαίτερα για προγραμματιστές που είναι εξοικειωμένοι με την παραδοσιακή τεχνολογία blockchain. Τα πρωτόκολλα που παρέχουν μόνο μερική παραγγελία, ενδέχεται να αντιμετωπίσουν περισσότερες δυσκολίες στην προσαρμογή τους στις υπάρχουσες υποδομές.
- 3) Ωριμότητα μηχανισμού συναίνεσης: Οι μηχανισμοί συναίνεσης που χρησιμοποιούνται σε DLT που βασίζονται σε DAG είναι συχνά νεότεροι και λιγότερο δοκιμασμένοι από αυτούς που χρησιμοποιούνται στα blockchains, με αποτέλεσμα να δημιουργείται αβεβαιότητα σχετικά με τη μακροπρόθεσμη σταθερότητα και ανθεκτικότητά τους έναντι των εξελισσόμενων απειλών δικτύου.

4) Πρόκληση προσβασιμότητας: Η προσβασιμότητα είναι κεντρικής σημασίας για την ακεραιότητα και την αποτελεσματική λειτουργία της δομής. Η έννοια της προσβασιμότητας εντός ενός DAG αναφέρεται στην ικανότητα ενός νέου μπλοκ να αναφέρεται σε παλαιότερες συναλλαγές ή μπλοκ. Αυτή η δυνατότητα έχει επιπτώσεις σε λειτουργίες, όπως η αφαίρεση παλιών δεδομένων για εξοικονόμηση χώρου και η λειτουργία ελαφρών πελατών, δηλαδή κόμβων που δεν αποθηκεύουν τα πλήρη δεδομένα του καθολικού (Raikwar et al. 2025).

Κεφάλαιο 7ο: Εφαρμογές - Περιπτώσεις Χρήσεις

Η ραγδαία ανάπτυξη του Διαδικτύου των Πραγμάτων (IoT) έχει μεταμορφώσει σημαντικά κλάδους όπως η υγειονομική περίθαλψη, οι μεταφορές και οι έξυπνες πόλεις, ενισχύοντας τις διαδικασίες συλλογής δεδομένων και λήψης αποφάσεων σε πραγματικό χρόνο (Ramírez-Gordillo et al 2025). Το blockchain έχει περισσότερες δυνατότητες από ένα απλό χρηματοοικονομικό εργαλείο. Ωστόσο, τα συμβατικά blockchain έχουν αποδειχθεί αναποτελεσματικά τόσο σε χρηματοοικονομικές εφαρμογές (π.χ. κρυπτονομίσματα) όσο και σε γενικές εφαρμογές (π.χ. έξυπνα συμβόλαια, ψηφιακά στοιχεία) και ανίκανα να χειριστούν αποτελεσματικά ασταθή δίκτυα



Εικόνα 7.1 Δείγμα διαδικασίας PowerGraph. Πηγή: Park and Kim (2019)

7.1 IoT συλλογή-ανταλλαγή δεδομένων

Οι τεχνολογίες Διαδικτύου των Πραγμάτων (IoT) και αισθητήρων έχουν επιτρέψει τη συλλογή δεδομένων με καταναμημένο τρόπο για ανάλυση και λήψη αποφάσεων βάσει τεκμηρίων. Ωστόσο, προκύπτουν ανησυχίες σχετικά με την ασφάλεια σχετικά με την πηγή, την εμπιστευτικότητα και την ακεραιότητα των δεδομένων. Η πιο κοινή μέθοδος προστασίας της μετάδοσης δεδομένων σε συστήματα αισθητήρων είναι η Ασφάλεια Επιπέδου Μεταφοράς (TLS) ή το αντίστοιχο datagram (DTLS) σήμερα, αλλά υπάρχει μια εναλλακτική επιλογή που βασίζεται στην Τεχνολογία Καταναμημένου Καθολικού (DLT) που υπόσχεται ισχυρή ασφάλεια, ευκολία χρήσης και δυνατότητες για ενσωμάτωση μεγάλης κλίμακας ετερογενών συστημάτων αισθητήρων. Ένα DLT όπως το IOTA Tangle προσφέρει μεγάλες δυνατότητες βελτίωσης της ανταλλαγής δεδομένων αισθητήρων. Αυτή η εργασία παρουσιάζει το L2Sec, ένα κρυπτογραφικό πρωτόκολλο που είναι σε θέση να ασφαλίσει δεδομένα που ανταλλάσσονται μέσω του IOTA Tangle. Αυτό το πρωτόκολλο είναι κατάλληλο για εφαρμογή σε συσκευές με περιορισμούς, όπως οι κοινές συσκευές IoT, οδηγώντας σε μεγαλύτερη επεκτασιμότητα. Τα πρώτα πειραματικά αποτελέσματα αποδεικνύουν την αποτελεσματικότητα της προσέγγισης και υποστηρίζουν την ενσωμάτωση ενός στοιχείου ασφαλείας υλικού για τη βελτίωση της συνολικής ασφάλειας του πρωτοκόλλου. Ο πηγαίος κώδικας L2Sec κυκλοφορεί ως αποθετήριο ανοιχτού κώδικα στο GitHub. Carelli et al 2022)

7.2. Ασφάλεια Δεδομένων μέσω του Tangle

Το Ίδρυμα IOTA ανέπτυξε δύο πρωτόκολλα L2 για τη δομή και την πλοήγηση δεδομένων μέσω του Tangle. Το Masked Authenticated Messaging (MAM) και το STREAMS To (MAM) λειτουργεί με την παλαιότερη έκδοση του IOTA Tangle και επιτρέπει σε οποιαδήποτε συσκευή να δημοσιεύει δεδομένα σε συναλλαγές μέσω του Tangle. Μπορεί να χρησιμοποιηθεί από μια συσκευή για την ασφαλή αγκύρωση μιας ροής δεδομένων στο Tangle, ενώ μόνο εξουσιοδοτημένες συσκευές είναι σε θέση να διαβάσουν, να ανακατασκευάσουν και να καταναλώσουν τη ροή δεδομένων. Το παλαιότερο IOTA Tangle εισήγαγε, για πρώτη φορά, την έννοια των συναλλαγών μηδενικής αξίας για την εγγραφή δεδομένων στο Tangle. Το πρωτόκολλο IOTA L1 είναι υπεύθυνο για τη συναλλαγή των δεδομένων, αλλά η συναλλαγή δεν προστατεύεται ή δεν ελέγχεται για τον σκοπό της επαλήθευσης της αυθεντικότητας των δεδομένων. Το MAM είναι το πρωτόκολλο L2 που παρέχει τον τρόπο σε μια συσκευή να προστατεύει και να δομεί ένα δίκτυο δεδομένων μέσω του Tangle και σε οποιεσδήποτε άλλες συσκευές να αποκρυπτογραφούν τη ροή δεδομένων και να επαληθεύουν την αυθεντικότητά της. Το MAM εισήγαγε την έννοια του καναλιού δεδομένων. Μόνο ο κάτοχος ενός καναλιού μπορεί να δημοσιεύσει δεδομένα σε ένα κανάλι και οποιαδήποτε κακόβουλη προσπάθεια ενός εχθρού να γράψει ψεύτικα δεδομένα μέσω του καναλιού ή να αναλάβει τον έλεγχο του καναλιού μπορεί εύκολα να ανιχνευθεί από συσκευές που έχουν εξουσιοδότηση να διαβάζουν και να καταναλώνουν τα δεδομένα του καναλιού. Τα κανάλια MAM είναι επομένως ένας απλός τρόπος επαλήθευσης ότι τα δεδομένα δημοσιεύθηκαν από μια δεδομένη συσκευή. Μόλις μια συσκευή δημοσιεύσει δεδομένα στο κανάλι της, λαμβάνει ένα αναγνωριστικό καναλιού, το οποίο είναι το αναγνωριστικό που επιτρέπει σε άλλη συσκευή να εγγραφεί στο κανάλι και να ανακτήσει τη ροή δεδομένων. Οποιαδήποτε δεδομένα σε ένα κανάλι συνοδεύονται από τις πληροφορίες της επόμενης διεύθυνσης που περιέχει τα επόμενα δεδομένα στο κανάλι (Carelli et al. 2022).

Διατίθενται λειτουργίες καναλιού Δημόσιου, Ιδιωτικού και Περιορισμένου Τύπου. Τα δημόσια κανάλια χρησιμοποιούν τη ρίζα ενός Merkle Tree ως διεύθυνση της συναλλαγής που περιέχει τα δεδομένα MAM, επομένως οποιαδήποτε συσκευή, δεδομένου του ID καναλιού, μπορεί να αποκρυπτογραφήσει δεδομένα χρησιμοποιώντας τη διεύθυνση ως κλειδί αποκρυπτογράφησης. Τα ιδιωτικά κανάλια χρησιμοποιούν το hash της ρίζας ενός Merkle Tree ως διεύθυνση της συναλλαγής που περιέχει τα δεδομένα MAM, επομένως μόνο η συσκευή με την αρχική ρίζα μπορεί να αποκρυπτογραφήσει τα δεδομένα. Τέλος, τα Περιορισμένα κανάλια προσθέτουν ένα προ-κοινόχρηστο συμμετρικό κλειδί εξουσιοδότησης στην ιδιωτική λειτουργία. Η διεύθυνση της συναλλαγής που περιέχει τα δεδομένα MAM είναι το hash του πλευρικού κλειδιού και της ρίζας του Merkle Tree, επομένως μόνο οι συσκευές με την αρχική ρίζα και το προ-κοινόχρηστο κλειδί μπορούν να αποκρυπτογραφήσουν τα δεδομένα.

Το STREAMS είναι ένα οργανωτικό εργαλείο για τη δομή και την πλοήγηση ασφαλών δεδομένων μέσω του Tangle. Ουσιαστικά, είναι ένα πλαίσιο για κρυπτογραφικές εφαρμογές ασφαλούς ανταλλαγής μηνυμάτων. Το STREAMS επιτρέπει σε οποιαδήποτε συσκευή να οργανώνει μηνύματα (δηλαδή, δεδομένα) σε μια ομοιόμορφη και διαλειτουργική δομή που υποστηρίζεται από το Tangle, το οποίο εγγυάται την ακεραιότητα και την αμετάβλητη δομή δεδομένων. Μια συσκευή, που ονομάζεται Publisher, μπορεί να στέλνει μηνύματα σε μια Ροή για όλους τους άλλους ή/και να περιορίζει την πρόσβαση σε μηνύματα και να την καθιστά ιδιωτική χρησιμοποιώντας κρυπτογράφηση δημόσιου κλειδιού. Οποιοσδήποτε άλλες συσκευές που επιθυμούν να καταναλώσουν μηνύματα, που ονομάζονται Συνδρομητές, μπορούν να εγγραφούν σε μια Ροή και να αντλούν πληροφορίες από το Tangle. Οι συνδρομητές μπορούν επίσης να συνεισφέρουν μηνύματα σε μια Ροή χρησιμοποιώντας διαφορετικούς τύπους τεχνικών διασταυρούμενης αναφοράς. Έτσι, οι Συνδρομητές μπορούν επίσης να δημοσιεύουν μη υπογεγραμμένα μηνύματα, σε αντίθεση με το MAM όπου μόνο ο κάτοχος του καναλιού μπορούσε να δημοσιεύσει δεδομένα. (Carelli et al. 2022). Επιπλέον, με τις νέες τεχνικές σύνδεσης, κάθε μήνυμα συνδέεται με ένα άλλο, επιτρέποντας τον τρόπο δημιουργίας σύνθετων δομών δεδομένων πιο ευέλικτων από την γραμμική αλυσίδα όπως στο MAM. Το STREAMS επανασχεδιάζει επίσης τους τύπους μηνυμάτων και προσθέτει διάφορους τύπους, καθιστώντας απλή τη δημοσίευση διαφορετικών μηνυμάτων στο ίδιο κανάλι και τη διάκρισή τους με βάση τις συγκεκριμένες κεφαλίδες τους. Τέλος, το STREAMS βελτιώνει τον έλεγχο πρόσβασης στο κανάλι, στην πραγματικότητα είναι δυνατό να εφαρμοστεί ένας διαφορετικός κρυπτογραφικός μηχανισμός σε κάθε μήνυμα με βάση τον τύπο του, για να δημιουργηθούν διαφορετικοί κανόνες ελέγχου πρόσβασης. Τόσο το MAM όσο και το STREAMS παρέχουν αποτελεσματικές λύσεις για τη δομή ασφαλών δεδομένων μέσω του Tangle. Οι γλώσσες προγραμματισμού που χρησιμοποιούνται για την ανάπτυξη αυτών των πρωτοκόλλων δεν είναι κατάλληλες για συσκευές IoT με περιορισμούς, οι οποίες αντιπροσωπεύουν την πλειονότητα των συσκευών που αναπτύσσονται σε εφαρμογές αισθητήρων πραγματικού κόσμου (Carelli et al 2022).

7.3 Υγειονομική Περίθαλψη και Διαδίκτυο των Πραγμάτων (IoT)

Η υγειονομική περίθαλψη έχει εξελιχθεί σημαντικά τα τελευταία χρόνια, κυρίως λόγω των εξελίξεων και της αυξανόμενης υιοθέτησης της τεχνολογίας στις διαδικασίες υγειονομικής περίθαλψης, όπως η συλλογή, η αποθήκευση, η διάγνωση και η θεραπεία δεδομένων. Η εμφάνιση του βιομηχανικού διαδικτύου των πραγμάτων (IoT) έχει εξελίξει περαιτέρω την ηλεκτρονική υγεία, διευκολύνοντας την ανάπτυξη συνδεδεμένων συστημάτων υγειονομικής περίθαλψης, τα οποία μπορούν να βελτιώσουν σημαντικά τη συνδεσιμότητα, την ορατότητα και τη διαλειτουργικότητα των δεδομένων, οδηγώντας σε βελτιωμένη ποιότητα υπηρεσιών που παρέχονται στους ασθενείς. Ωστόσο, τέτοιες τεχνολογικές

εξελίξεις συνοδεύονται από τους κινδύνους τους - υπάρχουν αυξανόμενες ανησυχίες σχετικά με την ασφάλεια και το απόρρητο των δεδομένων υγειονομικής περίθαλψης, ειδικά όταν συλλέγονται, κοινοποιούνται και υποβάλλονται σε επεξεργασία με χρήση συσκευών αισθητήρων αιχμής, οι οποίες επηρεάζουν την υιοθέτηση συστημάτων ηλεκτρονικής υγειονομικής περίθαλψης επόμενης γενιάς. Συγκεκριμένα, κατά τη μεταφορά δεδομένων front-end και back-end στην ανταλλαγή πληροφοριών υγείας (HIE), υπάρχει κίνδυνος ασφαλείας όσον αφορά την εμπιστευτικότητα, την ακεραιότητα, την αυθεντικοποίηση και τον έλεγχο πρόσβασης των δεδομένων λόγω των περιορισμένων δυνατοτήτων των συσκευών IoT που εμπλέκονται. Οι Abdullah et al. (2023) διερεύνησαν τη χρήση τεχνολογιών κατακευκαμένου καθολικού (DLT) για την αντιμετώπιση τέτοιων ανησυχιών ασφαλείας για τα αναδυόμενα συστήματα υγειονομικής περίθαλψης. Συγκεκριμένα, χρησιμοποίησαν την ανταλλαγή μηνυμάτων με μάσκα και έλεγχο ταυτότητας (MAM) μέσω του Tangle για να επιτύχουν ασφαλή κοινή χρήση δεδομένων εντός ενός συστήματος υγειονομικής περίθαλψης και να παρέχουν μια απόδειξη της εφαρμογής της προτεινόμενης προσέγγισης για την ασφάλεια των δεδομένων υγειονομικής περίθαλψης σε ένα συνδεδεμένο περιβάλλον IIoT. Επιπλέον, αξιολόγησαν και ανέλυσαν την επικοινωνία δεδομένων σε σχέση με τις μετρήσεις κρυπτογράφησης και αποτελεσματικότητας στον χρόνο συναλλαγής (Abdullah et al. 2023).

Οι Zhao et al. (2024) στην εργασία τους το 2024, σχεδίασαν ένα πρωτότυπο έξυπνης μάσκας για να παρακολουθεί την κατάσταση χρήσης μάσκας από άτομα, με σκοπό τον μετριασμό των επιπτώσεων ενός αερομεταφερόμενου ιού όπως ο COVID-19. Ο σχεδιασμός χρησιμοποίησε πρόσφατα αποτελέσματα από τη θεωρία ελέγχου ανάδρασης (feedback control) σε ένα κατακευκαμένο βιβλίο καταγραφής (distributed ledger) που έχουν αναπτυχθεί για την επιβολή της συμμόρφωσης με ψευδοανώνυμο τρόπο. Ο σχεδιασμός βασίζεται στη χρήση του κατακευκαμένου βιβλίου καταγραφής (IOTA). Η χρήση του IOTA Tangle που βασίζεται σε DLT, χρησιμεύει τόσο ως επίπεδο επικοινωνίας για τον αλγόριθμο ελέγχου όσο και ως ledger, εξασφαλίζοντας την ασφάλεια και την αμετάβλητη φύση των δεδομένων. Ο ελεγκτής χρησιμοποιείται για να σχηματίζει έναν βρόχο ανάδρασης για τη ρύθμιση του δικτύου. Μια προσομοίωση hardware-in-the-loop βασισμένη στην τοποθέτηση σε εσωτερικούς χώρους, σε συνδυασμό με προσομοιώσεις Monte-Carlo, αναπτύσσεται για να καταδείξει την αποτελεσματικότητα του σχεδιασμένου πρωτοτύπου.

7.4 Ψηφιακή ταυτότητα / έλεγχος πρόσβασης

Η μη εξουσιοδοτημένη πρόσβαση σε πόρους αποτελεί μια τυπική απειλή ασφάλειας στο Διαδίκτυο των Πραγμάτων (IoT), ενώ οι τεχνολογίες κατακευκαμένου καθολικού (π.χ., blockchain και IOTA) υπόσχονται πολλά στην αντιμετώπιση αυτής της απειλής. Παρόλο που τα συστήματα ελέγχου πρόσβασης IoT που βασίζονται σε blockchain είναι τα πιο δημοφιλή, υποφέρουν από αρκετούς σημαντικούς περιορισμούς, όπως το υψηλό χρηματικό κόστος και η χαμηλή απόδοση επεξεργασίας αιτημάτων πρόσβασης. Για να ξεπεραστούν αυτοί οι περιορισμοί, οι Zang et al (2021) πρότειναν ένα νέο σύστημα ελέγχου πρόσβασης IoT συνδυάζοντας την τεχνολογία IOTA χωρίς χρέωση και την τεχνολογία Κρυπτογράφησης Ciphertext-Policy Attribute-Based (CP-ABE), στο οποίο τα ABAC και CapBAC συνδυάζονται αξιοποιώντας την τεχνολογία CP-ABE. Χάρη στο CP-ABE, το σχέδιό αυτό ξεπερνά τα μειονεκτήματα που υπάρχουν στο προηγούμενο πλαίσιο με την ονομασία DCACI και παρέχει πιο ασφαλή, λεπτομερή και κλιμακωτό έλεγχο πρόσβασης. Οι Zang et al (2021) υλοποίησαν ένα πρωτότυπο σύστημα απόδειξης ιδέας χρησιμοποιώντας έξυπνα τηλέφωνα (Google Pixel 3XL) και μια εμπορική πύλη IoT (NEC EGW001). Αξιολόγησαν επίσης την απόδοση του προτεινόμενου σχήματος όσον αφορά την απόδοση επεξεργασίας αιτημάτων πρόσβασης. Τα πειραματικά

αποτελέσματα έδειξαν ότι το σχέδιό τους επιτρέπει στους κατόχους αντικειμένων να εξουσιοδοτούν δικαιώματα πρόσβασης σε μεγάλο αριθμό υποκειμένων σε περίπου 5 φορές μικρότερο χρόνο από το υπάρχον σχήμα ελέγχου πρόσβασης που ονομάζεται πλαίσιο ελέγχου πρόσβασης βασισμένο σε αποκεντρωμένες δυνατότητες χρησιμοποιώντας IOTA (DCACI), βελτιώνοντας σημαντικά την απόδοση επεξεργασίας αιτημάτων πρόσβασης Zhang, et al (2021). Επιπλέον, συζήτησαν την επεκτασιμότητα του σχεδίου τους λαμβάνοντας υπόψη έναν αυξημένο αριθμό χαρακτηριστικών και πολιτικών. Τα αποτελέσματα έδειξαν ότι ο χρόνος εκτέλεσης για κάθε λειτουργία είναι ανάλογος με τον αριθμό των χαρακτηριστικών που εμπλέκονται και ότι ο αριθμός των πολιτικών έχει μικρή επίδραση στον συνολικό χρόνο εκτέλεσης για τις περισσότερες λειτουργίες. Για τον έλεγχο της πρόσβασης σε έναν πόρο, ένα διακριτικό, το οποίο καταγράφει δικαιώματα πρόσβασης σε αυτόν τον πόρο, κρυπτογραφείται από την τεχνολογία CP-ABE και μεταφορτώνεται στο IOTA Tangle (δηλαδή, την υποκείμενη βάση δεδομένων του IOTA). Οποιοσδήποτε χρήστης μπορεί να ανακτήσει το κρυπτογραφημένο διακριτικό από το Tangle, ενώ μόνο όσοι μπορούν να αποκρυπτογραφήσουν αυτό το διακριτικό έχουν εξουσιοδότηση πρόσβασης στον πόρο. Με αυτόν τον τρόπο, το προτεινόμενο σχήμα επιτρέπει όχι μόνο κατανεμημένο, χωρίς χρέωση και κλιμακωτό έλεγχο πρόσβασης χάρη στο IOTA, αλλά και λεπτομερή έλεγχο πρόσβασης βασισμένο σε χαρακτηριστικά χάρη στο CP-ABE (Zhang, et al 2021).

7.5 Κινητικότητα και Διαλειτουργικότητα DLT

Η ανακάλυψη των Τεχνολογιών Κατανεμημένου Καθολικού (DLT) επέτρεψε την εμφάνιση και την εφαρμογή ενός ευρέος φάσματος ψηφιακών πλατφορμών σε Εικονικές Επιχειρήσεις (EE) οι οποίες συνεργάζονται για την παροχή ψηφιακών υπηρεσιών. Στο πλαίσιο των εικονικών επιχειρήσεων (VE), ερευνητές και επαγγελματίες έχουν αρχίσει να διερευνούν την ανάπτυξη της DLT για την αυτοματοποίηση της επεξεργασίας δεδομένων και την εφαρμογή αποφάσεων για την υποστήριξη της παροχής ψηφιακών υπηρεσιών. Το DLT έχει τη δυνατότητα να φέρει επανάσταση στο EE προσφέροντας διαφανή, αποκεντρωμένα, αξιόπιστα, με προέλευση δεδομένων, αξιόπιστα και ελέγξιμα χαρακτηριστικά. Η διαλειτουργικότητα του DLT είναι μία από τις προκλήσεις που εμποδίζουν την ευρεία υιοθέτηση των πλατφορμών DLT. Η εργασία του Bokolo (2022), παρουσιάζει μια πολυεπίπεδη αρχιτεκτονική που βοηθά στη διαλειτουργικότητα της DLT και των ψηφιακών πλατφορμών που βασίζονται στο IOTA Tangle. Υιοθετείται η μέθοδος της επιστήμης σχεδιασμού και πραγματοποιείται επίδειξη περίπτωσης για να δείξει πώς το IOTA Tangle επιτρέπει στο VE να παρέχει μια καινοτόμο εικονική πλατφόρμα πληρωμής περιουσιακών στοιχείων για απρόσκοπτη ηλεκτρική κινητικότητα ως υπηρεσία προς τους πελάτες. Το IOTA χρησιμοποιήθηκε ως πλατφόρμα DLT λόγω της ιχνηλασιμότητας δεδομένων, της αμετάβλητης φύσης και των χαρακτηριστικών προστασίας από παραβίαση που επιτρέπουν την επαλήθευση της ακεραιότητας των δεδομένων. Το IOTA προσφέρει ευελιξία και απόδοση για να υποστηρίξει μια αξιόπιστη ψηφιακή λύση. Τα ευρήματα από αυτήν τη μελέτη παρουσιάζουν μια πολυεπίπεδη αρχιτεκτονική που βοηθά το IOTA Tangle να υποβάλλει αιτήματα, να επικοινωνεί μεταξύ τους και να μοιράζεται δεδομένα μέσω της διεπαφής προγραμματισμού εφαρμογών RESTful ως πύλη με άλλες εξωτερικές ψηφιακές πλατφόρμες που αναπτύσσονται από το VE για την επίτευξη ενός διαλειτουργικού οικοσυστήματος. Η μελέτη του Bokolo (2023) παρουσιάζει ένα σενάριο περίπτωσης για να δείξει πώς το IOTA Tangle επιτρέπει στις εικονικές επιχειρήσεις να παρέχουν σύστημα πληρωμής εικονικών περιουσιακών στοιχείων για απρόσκοπτη ηλεκτρική κινητικότητα ως υπηρεσία στους πελάτες. Τα ευρήματα από τη μελέτη περίπτωσης μοντελοποιήθηκαν σε μια πολυεπίπεδη αρχιτεκτονική που δείχνει την εφαρμογή του IOTA Tangle για την παροχή ενός μηχανισμού που επιτρέπει την ανάπτυξη μιας καινοτόμου

πλατφόρμας πληρωμής εικονικών περιουσιακών στοιχείων που καθοδηγείται από RESTful APIs, βελτιώνοντας την εμπιστοσύνη στα δεδομένα με ασφαλή, αξιόπιστο και ελεγχόμενο τρόπο. Το IOTA Tangle χρησιμοποιήθηκε σε αυτή τη μελέτη ως η επιλεγμένη πλατφόρμα DLT, καθώς προσφέρει ευελιξία και απόδοση για να επιτρέψει ένα αξιόπιστο εικονικό περιβάλλον για εικονικές επιχειρήσεις. Αυτό το άρθρο αναπτύσσει ένα πλαίσιο αρχιτεκτονικής διακυβέρνησης βάσει σχεδιασμού που ορίζει τη διακυβέρνηση της DLT ως έναν συνδυασμό αρχιτεκτονικών στρωμάτων και διακυβέρνησης διαστάσεων της DLT. Χρησιμοποιείται η επιστήμη σχεδιασμού και το IOTA συνδυάζει μια DLT ανοιχτού κώδικα που χρησιμοποιεί ένα αποκεντρωμένο ασύγχρονο δίκτυο για να αξιολογήσει την εφαρμογή του αναπτυγμένου πλαισίου αρχιτεκτονικής διακυβέρνησης βάσει σχεδιασμού μέσω ποιοτικών συνεντεύξεων και έρευνας βιβλιογραφίας. Τα ευρήματα εντοπίζουν επίσης περιορισμούς που σχετίζονται με τη διακυβέρνηση λύσεων DLT και προτείνουν συστάσεις πολιτικής που θα χρησιμοποιηθούν ως κατευθυντήριες γραμμές για τους επαγγελματίες, ώστε να βελτιώσουν την υιοθέτηση της DLT με σκοπό την επιτάχυνση της ψηφιοποίησης της Εικονικής Πραγματικότητας. Αυτή η εργασία παρέχει ένα σημείο εκκίνησης για την εξερεύνηση της διαλειτουργικότητας DLT στον τομέα των εικονικών επιχειρήσεων

7.6 Αγορές δεδομένων

Τα τελευταία χρόνια, ο όγκος των δεδομένων που παράγονται από συσκευές IoT έχει αυξηθεί δραματικά. Η χρήση αυτών των δεδομένων μπορεί να βελτιώσει τη λήψη αποφάσεων στον δημόσιο και τον ιδιωτικό τομέα και να αυξήσει την παραγωγικότητα. Έχουν γίνει πολλές προσπάθειες για την ενίσχυση και την προσαρμογή των επιχειρήσεων ώστε να αξιοποιούν αυτά τα δεδομένα IoT. Μεταξύ αυτών, η εμπορία δεδομένων IoT είναι η πιο δημοφιλής προσέγγιση. Για το σκοπό αυτό, τα τρέχοντα έργα επικεντρώνονται επί του παρόντος στην ανάπτυξη αποκεντρωμένων αγορών δεδομένων για το IoT χρησιμοποιώντας blockchain και κρυπτονομίσματα. Οι Farahani & Shahriari (2022) εξερεύνησαν τη δυνατότητα δημιουργίας μιας αποκεντρωμένης αγοράς δεδομένων χρησιμοποιώντας το IOTA tangle και τις αλυσίδες έξυπνων συμβάσεων IOTA (αλυσίδες SC) και επιπλέον εξέτασαν τα πλεονεκτήματα μιας τέτοιας αρχιτεκτονικής όσον αφορά το κόστος, την επεκτασιμότητα και την ιδιωτικότητα σε σχέση με τα υπάρχοντα σχέδια. Συνέκριναν το παρουσιαζόμενο σύστημα με μια αγορά που έχει μόνο μία συγκεκριμένη αλυσίδα στο L2, και όλοι οι πωλητές και οι αγοραστές χρησιμοποιούν αυτήν την αλυσίδα και τα έξυπνα συμβόλαιά της για συναλλαγές μεταξύ τους. Σαφώς, αυτή η αγορά έχει υψηλότερη διακίνηση, αλλά η παρακολούθηση των επικοινωνιών θα ήταν πολύ πιο εύκολη για τον εισβολέα, με αποτέλεσμα το απόρρητο των χρηστών να τεθεί σε κίνδυνο και ο εισβολέας να μπορεί να αποκτήσει πληροφορίες σχετικά με τους χρήστες και τις συναλλαγές τους χρησιμοποιώντας μεθόδους παρόμοιες με τις επιθέσεις ανωνυμοποίησης. Επομένως, είναι σημαντικό να προστατευτεί το απόρρητο του χρήστη (ταυτότητα και τοποθεσία) για να αποτραπούν τέτοιες επιθέσεις. Οι Farahani & Shahriari (2022) στην εργασία τους, παρουσίασαν την αρχιτεκτονική μιας αποκεντρωμένης αγοράς δεδομένων που θα μπορούσε να ικανοποιήσει τις απαιτήσεις, όπως η ιδιωτικότητα, η επεκτασιμότητα και η οικονομικά αποδοτική απόδοση. Για το σκοπό αυτό, χρησιμοποίησαν τεχνολογίες όπως IOTA, IPFS και μια αποκεντρωμένη αρχή έκδοσης πιστοποιητικών.

7.7 Ηλεκτρονική ψηφοφορία με ShimmerEVM

Οι Maliki et al. (2024), πρότειναν ένα καινοτόμο ηλεκτρονικό σύστημα ψηφοφορίας που ενισχύει τη διαφάνεια, την ανωνυμία και την αξιοπιστία, με στόχο να φέρει επανάσταση τόσο στις παραδοσιακές όσο και στις υπάρχουσες μεθοδολογίες ηλεκτρονικής ψηφοφορίας. Το σύστημα αυξάνει την

προσβασιμότητα, την ασφάλεια και την αποτελεσματικότητα στην εκλογική διαδικασία. Προηγμένες τεχνολογίες ανάπτυξης ιστοσελίδων, συμπεριλαμβανομένων των NextJs, TailwindCSS, TypeScript, και JWT tokens, ενσωματώνονται για μια βελτιωμένη εμπειρία ηλεκτρονικής ψηφοφορίας. Αυτό το σύστημα χρησιμοποιεί κρυπτογράφηση και κρυπτογραφικά hashes για την ασφάλεια ευαίσθητων πληροφοριών, παράλληλα με έξυπνα συμβόλαια στο ShimmerEVM για να διασφαλίσει τη ανεξαρτησία και την αμετάβλητη φύση των δεδομένων, τα οποία είναι ζωτικής σημασίας για τη διατήρηση της ακεραιότητας των δεδομένων ψηφοφορίας και τον μετριασμό των κινδύνων χειραγώγησης της καταμέτρησης ψήφων. Ένα κρίσιμο χαρακτηριστικό του συστήματος είναι η ενεργοποίηση ενός βιομετρικού στοιχείου υλικού, απαραίτητου για την εγγραφή και τη συμμετοχή των ψηφοφόρων..

7.8 Κυκλική οικονομία / υποβολή δεδομένων IoT

Οι καταναεμημένες τεχνολογίες καθολικού (DLT) υποστηρίζουν συστήματα Ψηφιακής Κυκλικής Οικονομίας (DCE) που βασίζονται σε αποτελεσματικές ροές δεδομένων IoT. Το Shimmer, επιτρέπει απρόσκοπτες συναλλαγές με παράλληλη επικύρωση μέσω του μηχανισμού επιλογής συμβουλών. Σε τέτοια καθολικά βιβλία, ο κατακερματισμός μηνυμάτων προκαλεί μια αντιστάθμιση καθυστέρησης-απόδοσης καθώς το κόστος ανά μπλοκ αυξάνεται με την παράλληλη επικύρωση. Αυτή η απόδοση μειώνει την ενέργεια και τη συμφόρηση, υποστηρίζοντας τους στόχους του DCE. Ωστόσο, οι τελικοί χρήστες δεν μπορούν να ελέγξουν το μέγεθος του ωφέλιμου φορτίου ή το φορτίο δικτύου, οδηγώντας σε απρόβλεπτη καθυστέρηση και υψηλή χρήση CPU στις συσκευές υποβολής, αυξάνοντας την κατανάλωση ενέργειας. Οι υπάρχουσες προσεγγίσεις τροποποιούν κυρίως τα εσωτερικά του καθολικού βιβλίου, παραβλέποντας την προσαρμοστικότητα ή τις πολιτικές τελικού χρήστη. Οι Voulgaridis et al. (2025), παρουσίασαν το ABS-TD3, έναν προσαρμοστικό παράγοντα TD3 από offline σε online για το σωστό μέγεθος μπλοκ, τον μετριασμό της συμφόρησης και την καθυστέρηση επιβεβαίωσης στο Shimmer, ως μια πιθανή λύση για ομαλή ροή δεδομένων IoT σε πλαίσια DCE, διατηρώντας παράλληλα τις απρόσκοπτες αλληλεπιδράσεις των τελικών χρηστών. Συγκεκριμένα ανέλυσαν πραγματικά δεδομένα δικτύου Shimmer για να κατανοήσουν τους παράγοντες που επηρεάζουν την αλληλεπίδραση ενός χρήστη με το Shimmer, καθώς και να συνδυάσουν διαφορετικούς τύπους νέων μηχανισμών για αποτελεσματική μάθηση και προσαρμοστικότητα. Ανέπτυξαν μια βάση εκτός σύνδεσης με τους βασικούς ενσωματωμένους μηχανισμούς να είναι η Ενίσχυση Ανάκτησης, με το αντίστοιχο αποτέλεσμα να χρησιμοποιείται για τη διαμόρφωση προσαρμοστικών βαρών στη συνάρτηση ανταμοιβής. Δεύτερον, χρησιμοποίησαν τη βάση εκτός σύνδεσης ως τη μετάβαση σε ένα online περιβάλλον, το οποίο θα αλληλεπιδρά με το Shimmer DLT, και θα ενσωματώνεται με το PER και την εκθετική απόσβεση, και ένα μπόνους καινοτομίας βασισμένο σε αριθμήσεις. Τα αποτελέσματα της αξιολόγησης έδειξαν ότι ο σκοπός του μοντέλου επιτυγχάνεται αποτελεσματικά, σε σύγκριση με τέσσερα διαφορετικά σενάρια βάσης, δηλαδή πολιτικές μέγιστης, ελάχιστης, τυχαίας και σταθερού βάρους, με το μοντέλο να αποδεικνύει καλύτερους χρόνους υποβολής και βελτιστοποιημένη αξιοποίηση της CPU, ή μια ισορροπία μεταξύ των δύο παραγόντων. Κατά συνέπεια, ο προσαρμοστικός παράγοντας μεγέθους μπλοκ που υποστηρίζεται από RL θέτει τις αρχικές βάσεις για ομαλές ροές δεδομένων μεταξύ των περιουσιακών στοιχείων IoT και των καθολικών DCE (Voulgaridis et al. 2025),

7.9 Ασφαλής Διαχείριση Υλικολογισμικού

Με την αύξηση των συσκευών IoT που δημιουργούν μεγάλες ποσότητες δεδομένων ευαίσθητων στον χρήστη, το ακατάλληλο υλικολογισμικό βλάπτει την ασφάλεια και το απόρρητο των χρηστών. Οι πιο πρόσφατες οικιακές συσκευές ενσωματώνονται με λειτουργίες που διασφαλίζουν τη συμβατότητα με το IoT του έξυπνου σπιτιού. Ωστόσο, η εφαρμογή πολύπλοκων μηχανισμών ασφαλείας στο IoT περιορίζεται από τις δυνατότητες του υλικού της συσκευής, καθιστώντας τες ευάλωτες σε επιθέσεις. Τέτοιες επιθέσεις έχουν γίνει πρόσφατα συχνές. Για να αντιμετωπιστεί αυτό το ζήτημα, οι Wijesundara et al. (2024), ανέπτυξαν έναν ασφαλή μηχανισμό επαλήθευσης για το υλικολογισμικό που κυκλοφορεί από τον κατασκευαστή της συσκευής. Πρότειναν μια πύλη IoT για ασφαλή επαλήθευση και ενημέρωση υλικολογισμικού για έξυπνες οικιακές συσκευές IoT χρησιμοποιώντας το πρωτόκολλο IOTA MAM (Masked Authenticated Messaging) και ένα κατακευματισμένο σύστημα αρχείων με το πρωτόκολλο IPFS (Inter-Planetary File System). Αυτά τα δύο πρωτόκολλα επικοινωνίας διασφαλίζουν την αποκεντρωμένη επικοινωνία και την διανομή αρχείων υλικολογισμικού μεταξύ του προμηθευτή της συσκευής IoT και της τελικής συσκευής IoT. Το προτεινόμενο σχήμα, εκτελεί μια ασφαλή ενημέρωση υλικολογισμικού σε τελικές συσκευές IoT και διασφαλίζει την αυθεντικότητα και την ακεραιότητα του υλικολογισμικού. Προτάθηκαν δύο τύποι μεθόδων επικύρωσης για την ενημέρωση και την επικύρωση υλικολογισμικού. Υλοποίησαν το προτεινόμενο σχήμα χρησιμοποιώντας τρεις οντότητες, τον Προμηθευτή, την πύλη IoT και την τελική συσκευή IoT. Το σύστημα έδωσε πολλά υποσχόμενα αποτελέσματα στην εκτέλεση ασφαλών αυτοματοποιημένων ενημερώσεων υλικολογισμικού σε τελικές συσκευές IoT με πολύ χαμηλή υπολογιστική ισχύ. Η λειτουργικότητα του συστήματος υλοποιήθηκε χρησιμοποιώντας την εκτέλεση MAM της IOTA σε Raspberry Pi ως πύλη IoT μαζί με έναν μικροελεγκτή Wi-Fi ESP8266, αποδεικνύοντας την αποτελεσματικότητα της προσέγγισής μας. Η προτεινόμενη μεθοδολογία μπορεί να χρησιμοποιηθεί για ασφαλή διανομή υλικολογισμικού σε οικιακές εφαρμογές IoT. Wijesundara et al. (2024).

7.10 Συγκριτική αξιολόγηση περιπτώσεων χρήσης

Παρά τα αξιοσημείωτα επιτεύγματα στη δομή του blockchain, οι ερευνητές διαπίστωσαν πρόσφατα ότι οι παραδοσιακές δομές που βασίζονται σε αλυσίδες και οι τροποποιήσεις τους δεν μπορούσαν να ικανοποιήσουν τις ολοένα και πιο πολλές και ποικίλες απαιτήσεις των εφαρμογών blockchain. Ως εκ τούτου, οι αρχιτεκτονικές που βασίζονται σε Directed Acyclic Graph (DAG), άρχισαν να αναζωπυρώνουν το ενδιαφέρον τόσο του ακαδημαϊκού χώρου όσο και των βιομηχανιών (Wu et al. 2022). Τα DLT έχουν γίνει αρκετά δημοφιλή την τελευταία δεκαετία λόγω του ευρέος φάσματος εφαρμογών τους.

Το Internet of things (IoT) θεωρείται ως ένα νέο παράδειγμα που συνδέει φυσικά αντικείμενα με το Διαδίκτυο. Έτσι το IoT χρησιμοποίησε τον Ηλεκτρονικό Κώδικα Προϊόντος (EBC) μαζί με την Αναγνώριση Ραδιοσυχνότητας (RFID) για να παρακολουθήσει το δρομολόγιο των αντικειμένων στην αλυσίδα εφοδιασμού (Ashton, 2009). Η σύνδεση του φυσικού κόσμου με το Διαδίκτυο παίζει κρίσιμο ρόλο στη βελτίωση της ζωής των ανθρώπων, μετατρέποντας τις πόλεις σε «έξυπνες πόλεις» (Perera et al., 2017), τα σπίτια σε «έξυπνα σπίτια» (Doan et al., 2018) και τις πανεπιστημιούπολεις σε «έξυπνες πανεπιστημιούπολεις» (Angelis et al., 2015, Alsbouei, et al., 2019). Αυτά τα συστήματα ενισχύουν την εμπιστοσύνη και την ιδιωτικότητα στις ψηφιακές αλληλεπιδράσεις, με εφαρμογές στην υγειονομική περίθαλψη και τις έξυπνες πόλεις. (Ramírez-Gordillo et al. 2025)

Επιπλέον το IOTA 1.5 προσφέρει βελτιώσεις πρωτοκόλλου που επιτρέπουν τη λειτουργικότητα έξυπνων συμβολαίων, tokenized assets και stable coins, τα οποία θα μπορούσαν να επιτρέψουν νέες περιπτώσεις χρήσης για εφαρμογές IoT καταναλωτών και επιχειρήσεων, μια εφαρμογή

χαρακτηριστικών προϊόντος, όπως: επαναχρησιμοποιήσιμες διευθύνσεις, UTXO, νέο πορτοφόλι Firefly και νέες βιβλιοθήκες και Διεπαφή Προγραμματισμού Εφαρμογών (API) για μια βελτιωμένη εμπειρία προγραμματιστή (Alsbouï, et al 2023).

Επίσης μέσω μιας νέας τεχνολογίας όπως είναι τα Connected Autonomous Systems (CAS) αναμένεται να επιτευχθεί η συνεργατική αυτόνομη οδήγηση και τα έξυπνα συστήματα μεταφοράς (Wu et al 2023).

Τα συστήματα αυτά μπορούν να χρησιμοποιηθούν για τη δημιουργία ενός καινοτόμου ηλεκτρονικού συστήματος ψηφοφορίας που ενισχύει τη διαφάνεια, την ανωνυμία και την αξιοπιστία και αυξάνει την προσβασιμότητα, την ασφάλεια και την αποτελεσματικότητα στην εκλογική διαδικασία. Προηγμένες τεχνολογίες ανάπτυξης ιστοσελίδων, συμπεριλαμβανομένων των NextJs, TailwindCSS, TypeScript, και JWT tokens, ενσωματώθηκαν για μια βελτιωμένη εμπειρία ηλεκτρονικής ψηφοφορίας. Αυτό το σύστημα χρησιμοποιεί κρυπτογράφηση και κρυπτογραφικά hashes για την ασφάλεια ευαίσθητων πληροφοριών, παράλληλα με έξυπνα συμβόλαια στο ShimmerEVM για να διασφαλίσει τη ανεξαρτησία και την αμετάβλητη φύση των δεδομένων, που είναι ζωτικής σημασίας ώστε να αποφευχθούν οι κίνδυνοι χειραγώγησης κατά την καταμέτρηση των ψήφων (Maliki et al. 2024).

Κεφάλαιο 8ο: Προτεινόμενο πλαίσιο Επιλογής Αρχιτεκτονικής Shimmer /IOTA για εφαρμογές IoT

8.1 Σκοπός της προτεινόμενης προσέγγισης

Από τη συστηματική μελέτη της βιβλιογραφίας που πραγματοποιήθηκε στο πλαίσιο της παρούσας εργασίας προέκυψε ότι οι εφαρμογές που βασίζονται σε DAG-based Distributed Ledger Technologies δεν παρουσιάζουν ομοιόμορφες απαιτήσεις. Αντίθετα, οι διαφορετικές κατηγορίες εφαρμογών απαιτούν και διαφορετικούς συνδυασμούς χαρακτηριστικών, με αποτέλεσμα, η επιλογή κατάλληλης αρχιτεκτονικής να εξαρτάται από το είδος της εφαρμογής, τους διαθέσιμους υπολογιστικούς πόρους, την ευαισθησία των δεδομένων, την ανάγκη εκτέλεσης προγραμματιζόμενης λογικής και τις απαιτήσεις απόδοσης και διαλειτουργικότητας. Ως εκ τούτου οι προγραμματιστές χρειάζονται ένα πλαίσιο για να αξιολογούν ποιο DAG-based DLT ταιριάζει στις ανάγκες τους λαμβάνοντας υπόψη απόδοση, συνέπεια και τον συμβιβασμό αποκέντρωσης-ασφάλειας.

Η διαφοροποίηση αυτή είναι ιδιαίτερα σημαντική στο περιβάλλον του Internet of Things, όπου οι τελικές συσκευές μπορεί να διαθέτουν περιορισμένους υπολογιστικούς και ενεργειακούς πόρους, ενώ παράλληλα οι εφαρμογές μπορεί να απαιτούν υψηλό επίπεδο ασφάλειας και αξιόπιστη διαχείριση μεγάλων ροών δεδομένων, έλεγχο πρόσβασης, προστασία προσωπικών πληροφοριών ή αυτοματοποιημένη εκτέλεση ενεργειών. Για τον λόγο αυτό, η επιλογή μιας αρχιτεκτονικής DLT θα πρέπει να είναι πολύ προσεκτική και να μην λαμβάνει υπόψη γενικά χαρακτηριστικά, αλλά να γίνεται με βάση τις ιδιαίτερες απαιτήσεις της συγκεκριμένης εφαρμογής.

Από τη βιβλιογραφική ανασκόπηση προέκυψε επίσης ότι δεν υπάρχει μία μοναδική αρχιτεκτονική προσέγγιση κατάλληλη για όλες τις εφαρμογές. Με βάση λοιπόν τα ευρήματα της βιβλιογραφικής ανασκόπησης της παρούσας εργασίας, προτείνεται ένα πλαίσιο επιλογής αρχιτεκτονικής για εφαρμογές που αξιοποιούν το οικοσύστημα IOTA/Shimmer. Το πλαίσιο δεν αποτελεί νέο πρωτόκολλο συναίνεσης ούτε τροποποίηση του Shimmer. Αποτελεί ένα αρχιτεκτονικό πλαίσιο λήψης αποφάσεων που συνθέτει τα αποτελέσματα της βιβλιογραφικής ανασκόπησης και τα μετατρέπει σε συγκεκριμένες σχεδιαστικές επιλογές.

Το πλαίσιο αυτό αποσκοπεί στη σύνδεση των απαιτήσεων μιας εφαρμογής με την κατάλληλη αρχιτεκτονική διάταξη, και τους απαιτούμενους μηχανισμούς ασφάλειας.

Πχ. Εάν πρόκειται για μια εφαρμογή στην υγειονομική περίθαλψη υπάρχει η απαίτηση για ιδιωτικότητα καθόσον αφορά ευαίσθητα προσωπικά δεδομένα, ενώ εάν πρόκειται για μια εφαρμογή σε ηλεκτρονική ψηφοφορία υπάρχει η απαίτηση για αδιαβλητότητα καθόσον πρέπει να εξασφαλιστεί το αδιάβλητο της ψηφοφορίας. Για τον σκοπό αυτό προτείνονται τέσσερα αρχιτεκτονικά πρότυπα και ένας μηχανισμός αντιστοίχισης των απαιτήσεων της εφαρμογής με αυτά.

8.2 Βασικές απαιτήσεις εφαρμογών

Από την ανάλυση των περιπτώσεων χρήσης που εξετάστηκαν στην παρούσα εργασία προκύπτουν ορισμένες επαναλαμβανόμενες κατηγορίες απαιτήσεων. Επομένως η επιλογή της κατάλληλης αρχιτεκτονικής θα πρέπει να πραγματοποιείται με βάση αυτές τις κατηγορίες απαιτήσεων.

Η πρώτη κατηγορία αφορά τους **περιορισμένους υπολογιστικούς πόρους**. Σε εφαρμογές IoT, πολλές συσκευές δεν διαθέτουν την απαραίτητη υπολογιστική ισχύ ή μνήμη για να εκτελούν όλες τις λειτουργίες ενός πλήρους κόμβου DLT. Στις περιπτώσεις αυτές, η απευθείας αλληλεπίδραση με ένα

DLT μπορεί να δημιουργήσει πρόσθετο υπολογιστικό ή επικοινωνιακό κόστος. Για τον λόγο αυτό είναι απαραίτητη η χρήση ενδιάμεσων κόμβων, οι οποίοι αναλαμβάνουν μέρος της επικοινωνίας με το καταναμεμημένο καθολικό.

Η δεύτερη κατηγορία αφορά την **ιδιωτικότητα και την εμπιστευτικότητα των δεδομένων**. Η ακεραιότητα που παρέχεται από ένα καταναμεμημένο καθολικό δεν συνεπάγεται αυτομάτως και προστασία της ιδιωτικότητας. Εφαρμογές όπως η υγειονομική περίθαλψη, η διαχείριση ταυτότητας και οι αγορές δεδομένων απαιτούν πρόσθετους μηχανισμούς κρυπτογράφησης, ελέγχου πρόσβασης ή αποθήκευσης ευαίσθητων δεδομένων εκτός του καθολικού. Για τέτοιες εφαρμογές προτείνεται να μη θεωρείται το DLT ως γενικός χώρος αποθήκευσης του πλήρους περιεχομένου. Αντίθετα, μπορεί να χρησιμοποιείται για την καταγραφή hashes, αποδεικτικών ακεραιότητας, metadata ή άλλων στοιχείων επαλήθευσης, ενώ τα πραγματικά δεδομένα παραμένουν κρυπτογραφημένα ή αποθηκεύονται εκτός του DLT.

Η τρίτη κατηγορία αφορά την **ανάγκη εκτέλεσης προγραμματιζόμενης επιχειρησιακής λογικής**. Σε εφαρμογές όπως η ηλεκτρονική ψηφοφορία, η αυτοματοποίηση συμφωνιών ή οι αποκεντρωμένες αγορές δεδομένων, δεν αρκεί η απλή καταγραφή δεδομένων στο DLT. Απαιτείται η εκτέλεση έξυπνων συμβολαίων, γεγονός που οδηγεί σε αρχιτεκτονικές που αξιοποιούν το ShimmerEVM ή άλλο συμβατό Layer 2 περιβάλλον. Η επιλογή αυτή είναι συμβατή με την αρχιτεκτονική που ήδη αναλύθηκε στην εργασία, όπου το Stardust/Shimmer L1 λειτουργεί ως βασικό επίπεδο και οι αλυσίδες έξυπνων συμβολαίων μπορούν να ενσωματωθούν πάνω από αυτό.

Η τέταρτη κατηγορία αφορά τη **διαλειτουργικότητα**. Πολλές πραγματικές εφαρμογές δεν λειτουργούν αποκλειστικά πάνω σε ένα DLT αλλά πρέπει να επικοινωνούν με υφιστάμενες πληροφοριακές πλατφόρμες, APIs, βάσεις δεδομένων, συστήματα IoT και εξωτερικές υπηρεσίες. Κατά συνέπεια, η αρχιτεκτονική πρέπει να υποστηρίζει καθορισμένα σημεία διασύνδεσης μεταξύ του DLT και των εξωτερικών συστημάτων.

Η πέμπτη κατηγορία αφορά **τον ρυθμό παραγωγής και υποβολής δεδομένων**. Ειδικά για εφαρμογές που παράγουν συνεχείς ροές δεδομένων IoT, ιδιαίτερη σημασία έχουν οι απαιτήσεις απόδοσης, όπως ο χρόνος επιβεβαίωσης, η χρήση CPU, το μέγεθος των υποβαλλόμενων δεδομένων, η συχνότητα υποβολής και η συνολική επιβάρυνση του δικτύου.

8.3 Προτεινόμενα αρχιτεκτονικά πρότυπα

Με βάση τα παραπάνω κριτήρια, η παρούσα εργασία προτείνει τέσσερα βασικά αρχιτεκτονικά πρότυπα.

8.3.1 Πρότυπο A: Άμεση καταγραφή το Layer 1

Το πρώτο πρότυπο αφορά εφαρμογές στις οποίες η βασική απαίτηση είναι η καταγραφή, η επαλήθευση ή η αγκύρωση δεδομένων στο καταναμεμημένο καθολικό. Σε αυτή την περίπτωση, η εφαρμογή επικοινωνεί απευθείας με έναν κόμβο IOTA/Shimmer μέσω του αντίστοιχου SDK ή API.

Η βασική αρχιτεκτονική είναι:

Εφαρμογή ή IoT συσκευή → SDK/API → Shimmer/IOTA node → DAG/Tangle

Η εφαρμογή δημιουργεί τα δεδομένα και μέσω του κατάλληλου SDK ή API τα υποβάλλει σε έναν κόμβο του δικτύου. Το πρότυπο αυτό είναι κατάλληλο όταν η τελική συσκευή διαθέτει επαρκείς πόρους για να επικοινωνεί άμεσα με το DLT και δεν απαιτείται πολύπλοκη επιχειρησιακή λογική ή εκτέλεση έξυπνων συμβολαίων και όταν η συσκευή διαθέτει επαρκείς πόρους. Το βασικό πλεονέκτημα είναι η απλότητα της αρχιτεκτονικής, καθώς περιορίζεται ο αριθμός των ενδιάμεσων

επιπέδων. Ωστόσο, η λύση δεν είναι κατάλληλη για κάθε IoT συσκευή, ιδιαίτερα όταν υπάρχουν αυστηροί ενεργειακοί ή υπολογιστικοί περιορισμοί.

8.3.2 Πρότυπο B: Gateway-assisted αρχιτεκτονική

Το δεύτερο πρότυπο αφορά συσκευές IoT με περιορισμένους πόρους. Στην περίπτωση αυτή, η τελική συσκευή δεν επικοινωνεί απευθείας με το DLT, οπότε προτείνεται ένα δεύτερο πρότυπο, στο οποίο εισάγεται ενδιάμεσο IoT gateway.

Η γενική αρχιτεκτονική είναι:

IoT συσκευή → IoT Gateway → SDK/API → IOTA/Shimmer node → DAG /Tangle

Στην περίπτωση αυτή οι αισθητήρες δεν χρειάζεται να αναλάβουν ολόκληρη τη διαδικασία επικοινωνίας με το DLT. Το gateway μπορεί να αναλαμβάνει την προεπεξεργασία των δεδομένων, την κρυπτογράφηση, επαλήθευση, ομαδοποίηση δεδομένων, τη δημιουργία των κατάλληλων μηνυμάτων και την επικοινωνία με τον κόμβο.

Με αυτόν τον τρόπο μειώνεται η επιβάρυνση των τελικών συσκευών. Το πρότυπο B προτείνεται κυρίως για δίκτυα αισθητήρων, smart-city εφαρμογές, βιομηχανικά IoT περιβάλλοντα και άλλες εφαρμογές στις οποίες μεγάλος αριθμός ελαφρών συσκευών παράγει συνεχώς δεδομένα.

8.3.3 Πρότυπο Γ: Υβριδική αρχιτεκτονική προστασίας ιδιωτικότητας

Το τρίτο πρότυπο αφορά εφαρμογές που επεξεργάζονται ευαίσθητα δεδομένα. Σε αυτές τις περιπτώσεις δεν προτείνεται η αποθήκευση ολόκληρου του περιεχομένου στο κατακευματισμένο καθολικό.

Η βασική αρχιτεκτονική είναι:

IoT Device → Gateway/Application → Κρυπτογράφηση → Off-chain Αποθήκευση

και παράλληλα:

Hash / Metadata / Proof → Shimmer/IOTA → DAG/Tangle

Στο συγκεκριμένο πρότυπο γίνεται διαχωρισμός μεταξύ δεδομένων και αποδεικτικών στοιχείων για τα δεδομένα. Με αυτόν τον τρόπο, το DLT χρησιμοποιείται για την επαλήθευση της ακεραιότητας, της προέλευσης ή των δικαιωμάτων πρόσβασης, ενώ τα ευαίσθητα δεδομένα παραμένουν κρυπτογραφημένα ή αποθηκευμένα εκτός του καθολικού. Το πρότυπο αυτό είναι περισσότερο κατάλληλο για εφαρμογές υγειονομικής περίθαλψης, ψηφιακής ταυτότητας και αποκεντρωμένων αγορών δεδομένων και γενικότερα εφαρμογές στις οποίες η εμπιστευτικότητα αποτελεί βασική απαίτηση.

8.3.4 Πρότυπο Δ: Smart-contract και Layer 2 αρχιτεκτονική

Το τέταρτο πρότυπο αφορά εφαρμογές που απαιτούν εκτέλεση επιχειρησιακής λογικής μέσω έξυπνων συμβολαίων.

Η γενική αρχιτεκτονική είναι:

Χρήστης / IoT Application → dApp → Smart Contract → ShimmerEVM / L2 → Shimmer L1

Σε αυτή την περίπτωση, το Layer 1 παρέχει το βασικό επίπεδο του κατακευματισμένου καθολικού, ενώ το ShimmerEVM επιτρέπει την εκτέλεση έξυπνων συμβολαίων και εφαρμογών συμβατών με το EVM. Το πρότυπο αυτό είναι κατάλληλο για εφαρμογές όπως ηλεκτρονική ψηφοφορία, αυτοματοποιημένος έλεγχος πρόσβασης, αγορές δεδομένων και άλλες εφαρμογές που απαιτούν προγραμματιζόμενους κανόνες.

8.4 Προτεινόμενη διαδικασία λήψης απόφασης για την επιλογή αρχιτεκτονικής

Η βασική συνεισφορά του πλαισίου δεν περιορίζεται στην παρουσίαση των τεσσάρων προτύπων. Με βάση τα παραπάνω πρότυπα, προτείνεται μια διαδικασία επιλογής που ξεκινά από τις απαιτήσεις της εφαρμογής.

Αρχικά γίνεται έλεγχος πόρων συσκευής. Εξετάζεται εάν η τελική IoT συσκευή διαθέτει επαρκείς υπολογιστικούς και ενεργειακούς πόρους. Εάν οι πόροι είναι περιορισμένοι, προτείνεται η χρήση gateway-assisted αρχιτεκτονικής. επιλέγεται δηλαδή κατά προτεραιότητα το **Πρότυπο Β (Gateway-Assisted)**.

Στη συνέχεια γίνεται έλεγχος ευαισθησίας δεδομένων. Εξετάζεται εάν η εφαρμογή διαχειρίζεται ευαίσθητα προσωπικά δεδομένα, ιατρικά ή άλλα. Εάν η απάντηση είναι θετική, προτείνεται η χρήση υβριδικής αρχιτεκτονικής με κρυπτογράφηση, μηχανισμούς ελέγχου πρόσβασης και περιορισμένη αποθήκευση δεδομένων στο DLT. Τότε επιλέγεται το **Πρότυπο Γ (Privacy-Preserving Hybrid)**.

Το επόμενο βήμα αφορά τον έλεγχο ανάγκης για έξυπνα συμβόλαια. Εάν απαιτείται εκτέλεση προγραμματιζόμενης επιχειρησιακής λογικής, προτείνεται η χρήση ShimmerEVM ή αντίστοιχου Layer 2 περιβάλλοντος. Σε αυτήν την περίπτωση επιλέγεται το **Πρότυπο Δ (Smart Contract/L2)**.

Στο επόμενο βήμα γίνεται απλή καταγραφή δεδομένων. Εάν δεν ισχύουν οι προηγούμενες απαιτήσεις και ο βασικός στόχος είναι η ακεραιότητα ή η καταγραφή δεδομένων, μπορεί να χρησιμοποιηθεί το **Πρότυπο Α (Direct L1)**.

Τέλος, γίνεται έλεγχος απόδοσης και διαλειτουργικότητας. Εξετάζονται οι απαιτήσεις απόδοσης και διαλειτουργικότητας, οι οποίες μπορεί να οδηγήσουν σε προσαρμογή του τρόπου υποβολής δεδομένων, χρήση APIs, middleware ή πρόσθετων μηχανισμών βελτιστοποίησης.

Το σημαντικό είναι ότι τα πρότυπα δεν είναι αμοιβαία αποκλειόμενα. Για παράδειγμα, μια εφαρμογή υγείας μπορεί να συνδυάζει το Πρότυπο Β λόγω περιορισμένων IoT αισθητήρων και το Πρότυπο Γ λόγω ευαίσθητων δεδομένων.

8.5 Πίνακας αντιστοίχισης απαιτήσεων και αρχιτεκτονικής

Απαίτηση εφαρμογής	Προτεινόμενο πρότυπο	Κύρια αρχιτεκτονική επιλογή
Περιορισμένοι πόροι συσκευής	Πρότυπο Β	Gateway-assisted
Απλή καταγραφή / ακεραιότητα δεδομένων	Πρότυπο Α	Άμεση χρήση L1
Ευαίσθητα προσωπικά δεδομένα	Πρότυπο Γ	Hybrid / off-chain
Smart contracts	Πρότυπο Δ	ShimmerEVM / L2
Υψηλή διαλειτουργικότητα	Πρότυπο Β ή Δ	APIs / middleware / EVM
Μεγάλος ρυθμός IoT δεδομένων	Πρότυπο Α ή Β	Adaptive/aggregated submission

Απαίτηση εφαρμογής	Προτεινόμενο πρότυπο	Κύρια αρχιτεκτονική επιλογή
Μεγάλος αριθμός αισθητήρων	B	Gateway + aggregation
Μεγάλα αρχεία	Πρότυπο Γ	Off-chain storage + DLT proof
Έλεγχος πρόσβασης	Γ ή Δ	Privacy layer / smart contract
Αυτοματοποιημένη επιχειρησιακή λογική	Δ	Smart contracts

Η παραπάνω ποιοτική αντιστοίχιση δεν αποτελεί πλήρη πειραματική επικύρωση του πλαισίου. Παρέχει, ωστόσο, ένδειξη ότι οι προτεινόμενες κατηγορίες και τα κριτήρια επιλογής αντανακλούν τα αρχιτεκτονικά χαρακτηριστικά που εμφανίζονται σε πραγματικές ερευνητικές εφαρμογές.

8.6 Ποιοτική αξιολόγηση του προτεινόμενου πλαισίου

Η καταλληλότητα του προτεινόμενου πλαισίου μπορεί να εξεταστεί συγκρίνοντάς το με επιλεγμένες περιπτώσεις χρήσης της βιβλιογραφίας. Το πλαίσιο μπορεί να εφαρμοστεί σε χαρακτηριστικές κατηγορίες εφαρμογών που εξετάστηκαν στην προηγούμενη βιβλιογραφική ανάλυση.

Περίπτωση 1 – IoT αισθητήρες Ένα δίκτυο αποτελείται από μεγάλο αριθμό αισθητήρων που παράγουν συνεχείς μετρήσεις. Οι συσκευές έχουν περιορισμένους υπολογιστικούς πόρους και η εφαρμογή δεν απαιτεί smart contracts. Στην περίπτωση αυτή το framework οδηγεί στην επιλογή gateway-assisted αρχιτεκτονικής.

Με βάση τον πίνακα 8.5 : **περιορισμένοι πόροι → Πρότυπο B → Gateway-Assisted Architecture.**

Το gateway μπορεί να συλλέγει τις μετρήσεις, να πραγματοποιεί βασική επεξεργασία ή ομαδοποίηση και να αναλαμβάνει την επικοινωνία με το DLT.

Περίπτωση 2 – Δεδομένα υγείας Σε μια εφαρμογή απομακρυσμένης παρακολούθησης ασθενών, οι IoT συσκευές συλλέγουν ευαίσθητες πληροφορίες υγείας. Στην περίπτωση αυτή, οι απαιτήσεις εμπιστευτικότητας και ελέγχου πρόσβασης οδηγούν στην επιλογή υβριδικής αρχιτεκτονικής προστασίας ιδιωτικότητας.

Με βάση τον πίνακα 8.5 **ευαίσθητα δεδομένα → Πρότυπο Γ → Privacy-Preserving Hybrid Architecture.**

Τα πραγματικά δεδομένα διατηρούνται κρυπτογραφημένα εκτός του DLT, ενώ το DLT χρησιμοποιείται για την καταγραφή αποδεικτικών ακεραιότητας ή σχετικών metadata.

Περίπτωση 3 – Ηλεκτρονική ψηφοφορία

Σε ένα σύστημα ηλεκτρονικής ψηφοφορίας απαιτείται εκτέλεση κανόνων σχετικά με την υποβολή και επεξεργασία των ψήφων. Στην περίπτωση αυτή η διαχείριση της διαδικασίας μέσω έξυπνων συμβολαίων οδηγεί στην επιλογή του προτύπου Layer 2 / ShimmerEVM. Η αρχιτεκτονική αυτή είναι συμβατή με την υλοποίηση ηλεκτρονικής ψηφοφορίας που εξετάστηκε στην παρούσα εργασία (Κεφάλαιο 7).

Η απαίτηση προγραμματιζόμενης λογικής σύμφωνα με τον πίνακα 8.5 οδηγεί στο:
smart-contract functionality → Πρότυπο Δ → ShimmerEVM/L2.

8.7 Συμβολή του προτεινόμενου πλαισίου

Η βασική συνεισφορά του προτεινόμενου πλαισίου είναι ότι οργανώνει τα ευρήματα της συστηματικής βιβλιογραφικής ανασκόπησης σε μια ενιαία διαδικασία λήψης αποφάσεων αρχιτεκτονικής επιλογής.

Αντί να αντιμετωπίζονται η αρχιτεκτονική, οι μηχανισμοί συναίνεσης, η ασφάλεια και οι περιπτώσεις χρήσης ως ανεξάρτητα θέματα, το προτεινόμενο πλαίσιο επιχειρεί να τα συνδέσει με βάση την εφαρμογή και μέσω αυτού προτείνεται η αρχιτεκτονική να προσαρμόζεται στις πραγματικές απαιτήσεις της εφαρμογής. Με αυτόν τον τρόπο διακρίνονται τέσσερις διαφορετικές στρατηγικές: άμεση αξιοποίηση του Layer 1, χρήση gateway, υβριδική αρχιτεκτονική προστασίας δεδομένων και αξιοποίηση Layer 2/smart contracts.

Η προσέγγιση αυτή συνδέει τρεις διαστάσεις που εξετάστηκαν χωριστά στα προηγούμενα κεφάλαια της εργασίας: **την αρχιτεκτονική του DLT, τις τεχνικές προκλήσεις και τις περιπτώσεις χρήσης.**

Το πλαίσιο δεν προτείνεται ως καθολική ή οριστική λύση. Αντίθετα, το πλαίσιο λειτουργεί ως δομημένη σύνδεση μεταξύ των αποτελεσμάτων της βιβλιογραφικής ανασκόπησης και μιας συγκεκριμένης αρχιτεκτονικής πρότασης. Με αυτόν τον τρόπο, μπορεί να χρησιμοποιηθεί ως αρχικό εργαλείο αξιολόγησης για ερευνητές ή σχεδιαστές εφαρμογών που εξετάζουν την αξιοποίηση του οικοσυστήματος IOTA/Shimmer, και μπορεί να επεκταθεί στο μέλλον με ποσοτικές μετρήσεις και πειραματική αξιολόγηση.

8.8 Περιορισμοί και μελλοντική επέκταση

Ο βασικός περιορισμός της προτεινόμενης προσέγγισης είναι ότι η αξιολόγησή της βασίζεται κυρίως σε ποιοτική ανάλυση των εργασιών που περιελήφθησαν στη βιβλιογραφική ανασκόπηση και όχι σε πειραματική υλοποίηση.

Επιπλέον, η βιβλιογραφία που αφορά άμεσα το Shimmer Network είναι πιο περιορισμένη σε σχέση με τη γενικότερη βιβλιογραφία για IOTA και DAG-based DLT. Κατά συνέπεια, ορισμένες από τις αρχιτεκτονικές κατηγορίες του πλαισίου βασίζονται σε συμπεράσματα από το ευρύτερο οικοσύστημα IOTA και από DAG-based αρχιτεκτονικές.

Μελλοντική εργασία θα μπορούσε να επεκτείνει το πλαίσιο με ποσοτικούς δείκτες, όπως χρόνος επιβεβαίωσης, κατανάλωση CPU, ενεργειακό κόστος, μέγεθος δεδομένων και υπολογιστικό overhead. Με αυτόν τον τρόπο η επιλογή μεταξύ των τεσσάρων αρχιτεκτονικών προτύπων θα μπορούσε να βασίζεται όχι μόνο σε ποιοτικά κριτήρια αλλά και σε μετρήσιμα δεδομένα. Επιπλέον, το πλαίσιο θα μπορούσε να αξιολογηθεί μέσω πραγματικής υλοποίησης διαφορετικών εφαρμογών σε Shimmer/IOTA ή και σε άλλα DAG-based DLT συστήματα. Θα μπορούσε να αναπτυχθεί ένα πραγματικό πρωτότυπο για κάθε αρχιτεκτονικό πρότυπο, να πραγματοποιηθεί συγκριτική πειραματική αξιολόγηση, δοκιμές ασφαλείας κ.λπ. Κάτι τέτοιο θα επέτρεπε την ποσοτική επικύρωση του προτεινόμενου πλαισίου και την περαιτέρω προσαρμογή του σε διαφορετικές κατηγορίες IoT εφαρμογών.

Κεφάλαιο 9ο: Συμπεράσματα

Αυτή η μελέτη επικύρωσε την αποτελεσματικότητα της χρήσης αποκεντρωμένων μοντέλων ταυτότητας που υποστηρίζονται από την αρχιτεκτονική DAG της IOTA για την ενίσχυση της ασφάλειας, της επεκτασιμότητας και της ιδιωτικότητας σε οικοσυστήματα IoT, αξιοποιώντας τις μοναδικές ιδιότητες του IOTA, όπως οι αβλαβείς συναλλαγές και η υψηλή επεκτασιμότητα.

Τα αποτελέσματα υπογραμμίζουν τις δυνατότητες των λύσεων που βασίζονται στο IOTA να προωθήσουν το όραμα ενός ασφαλούς, ενδυναμωμένου από τον χρήστη Διαδικτύου, ανοίγοντας το δρόμο για περαιτέρω καινοτομίες στις αποκεντρωμένες τεχνολογίες και τις εφαρμογές τους σε οικοσυστήματα IoT.

Αυτή η ισορροπία είναι ιδιαίτερα σημαντική για το IoT, όπου μεγάλες ποσότητες μη κρίσιμων δεδομένων πρέπει να αποθηκεύονται εκτός αλυσίδας, ενώ τα απαραίτητα μεταδεδομένα και οι κρυπτογραφικές αποδείξεις διατηρούνται εντός της αλυσίδας για επικύρωση και αξιοπιστία.

Η χρήση αυτών των συστημάτων ανοίγει τον δρόμο για πιο καινοτόμες και προσανατολισμένες στον χρήστη εφαρμογές σε διάφορους τομείς, συμπεριλαμβανομένων των έξυπνων πόλεων, της υγειονομικής περίθαλψης και της διαχείρισης της εφοδιαστικής αλυσίδας.

Παρά τα υποσχόμενα αποτελέσματα, τα συστήματα αυτά αντιμετωπίζουν και αρκετές προκλήσεις, συμπεριλαμβανομένων των υψηλών υπολογιστικών απαιτήσεων των κρυπτογραφικών λειτουργιών σε συσκευές χαμηλής ισχύος και την ανάγκη για καλύτερη ενσωμάτωση πρωτοκόλλων συναίνεσης.

Η μελλοντική έρευνα θα πρέπει να επικεντρωθεί στη βελτιστοποίηση των κρυπτογραφικών αλγορίθμων για περιβάλλοντα με περιορισμένους πόρους, στην διερεύνηση της ενσωμάτωσης προηγμένων πρωτοκόλλων και στην επέκταση των αξιολογήσεων επεκτασιμότητας σε ποικίλα περιβάλλοντα IoT. Η μελλοντική έρευνα θα πρέπει να αντιμετωπίσει προκλήσεις, εξερευνώντας άλλα πρωτόκολλα επικοινωνίας και βελτιστοποιώντας τις κρυπτογραφικές λειτουργίες για συσκευές IoT χαμηλής ισχύος. Επιπλέον, είναι απαραίτητη μια ανάλυση κόστους-οφέλους μόνιμων έναντι μη μόνιμων κόμβων για την αποθήκευση αρχείων ταυτότητας, λαμβάνοντας υπόψη τους συμβιβασμούς μεταξύ της σταθερότητας και του υψηλότερου κόστους των μόνιμων κόμβων έναντι της ευελιξίας και του χαμηλότερου κόστους των μη μόνιμων κόμβων.

Κεφάλαιο 10ο: Βιβλιογραφία

Προδημοσιεύσεις

- [1] C. Cachin and M. Vukolić, “Blockchain Consensus Protocols in the Wild,” arXiv preprint arXiv:1707.01873. 2017.
- [2] N. Kannengießer, S. Lins, T. Dehling, and A. Sunyaev, “Mind the Gap: Trade-Offs Between Distributed Ledger Technology Characteristics,” arXiv preprint arXiv:1906.00861. 2019.
- [3] F. Keramat, J. P. Queralta, and T. Westerlund, “Partition-Tolerant and Byzantine-Tolerant Decision-Making for Distributed Robotic Systems with IOTA and ROS 2,” arXiv preprint arXiv:2208.13467. 2022.
- [4] M. Raikwar, “A Review on Privacy in DAG-Based DLTs,” arXiv preprint arXiv:2504.15233. 2025.
- [5] C. Zhang, Z. Luo, R. Ramesh, and A. Kate, “Optimal Sharding for Scalable Blockchains with Deconstructed SMR,” arXiv preprint arXiv:2406.08252. 2025.
- [6] G. Zhang, Y. Mao, S. Zhang, S. Motepalli, F. Pan, and H.-A. Jacobsen, “V-Guard: An Efficient Permissioned Blockchain for Achieving Consensus under Dynamic Memberships in V2X Networks,” arXiv preprint arXiv:2301.06210. 2023.

Δημοσιεύσεις: Περιοδικά και Συνέδρια με κρίση

- [1] S. Ahuja, R. Johari, and C. Khokhar, “IoT: Internet of Things Application,” in Proc. 2nd Int. Conf. Computer and Communication Technologies, vol. 381, Advances in Intelligent Systems and Computing, Springer, doi: 10.1007/978-81-322-2526-3_26. 2016.
- [2] S. Abdullah, J. Arshad, M. M. Khan, M. Alazab, and K. Salah, “PRISED Tangle: A Privacy-Aware Framework for Smart Healthcare Data Sharing Using IOTA Tangle,” Complex & Intelligent Systems, vol. 9, pp. 3023–3041, doi: 10.1007/s40747-021-00610-8. 2023.
- [3] M. A. Al Mamun, “Real-Time Integration of IoT Sensor and IOTA Tangle for Securing IoT Infrastructure,” M.S. thesis. 2021.
- [4] R. Alexander, IOTA – Introduction to the Tangle Technology: Everything You Need to Know About the Revolutionary Blockchain Alternative, ISBN: 978-1-9804-1887-0. 2018.
- [5] T. Alsboui, Y. Qin, and R. Hill, “Enabling Distributed Intelligence in the Internet of Things Using the IOTA Tangle Architecture,” in Proc. 4th Int. Conf. Internet of Things, Big Data and Security (IoTBDs), pp. 392–398, doi: 10.5220/0007751403920398. 2019.
- [6] T. Alsboui, Y. Qin, R. Hill, and H. Al-Aqrabi, “Towards a Scalable IOTA Tangle-Based Distributed Intelligence Approach for the Internet of Things,” in Proc. Computing Conf. (SAI 2020), vol. 2, Advances in Intelligent Systems and Computing, vol. 1229, pp. 487–501, doi: 10.1007/978-3-030-52246-9_35. 2020.
- [7] T. Alsboui, Y. Qin, R. Hill, and H. Al-Aqrabi, “Enabling Distributed Intelligence for the Internet of Things with IOTA and Mobile Agents,” Computing. 2020.
- [8] T. A. Alsboui, M. Hussain, H. Al-Aqrabi, R. Hill, and M. Hijjawi, “A Scalable Decentralized and Lightweight Access Control Framework Using IOTA Tangle for the Internet of Things,” in Proc. 8th Int. Conf. Internet of Things, Big Data and Security (IoTBDs), pp. 178–185, doi: 10.5220/0011963600003482. 2023.
- [9] E. D. Angelis, A. Ciribini, L. Tagliabue, and M. Paneroni, “The Brescia Smart Campus Demonstrator: Renovation Toward a Zero-Energy Classroom Building,” Procedia Engineering, vol. 118, pp. 735–743. 2015.
- [10] P. Arthurs, L. Gillam, P. Krause, N. Wang, K. Halder, and A. Mouzakitis, “A Taxonomy and Survey of Edge Cloud Computing for Intelligent Transportation Systems and Connected Vehicles,” IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 7, pp. 6206–6221. 2022.

- [11] K. Ashton, “That ‘Internet of Things’ Thing,” *RFID Journal*. 2009.
- [12] B. Anthony Jnr., “Exploring Interoperability of Distributed Ledger and Decentralized Technology Adoption in Virtual Enterprises,” *Information Systems and e-Business Management*, vol. 20, pp. 685–718, doi: 10.1007/s10257-022-00561-8. 2022.
- [13] B. Anthony Jnr., “Inclusive and Safe Mobility Needs of Senior Citizens: Implications for Age-Friendly Cities and Communities,” *Urban Science*, vol. 7, no. 4, Art. no. 103, doi: 10.3390/urbansci7040103. 2023.
- [14] M. Baboi, “Security of Consensus Mechanisms in Blockchain,” *Romanian Cyber Security Journal*, vol. 5, no. 2, Fall. 2023.
- [15] S. Bano, A. Sonnino, M. Al-Bassam, S. Azouvi, P. McCorry, S. Meiklejohn, and G. Danezis, “SoK: Consensus in the Age of Blockchains,” in *Proc. 1st ACM Conf. Advances in Financial Technologies (AFT ’19)*, pp. 183–198, doi: 10.1145/3318041.335545. 2019.
- [16] B. Bellaj, A. Ouaddah, E. Bertin, N. Crespi, and A. Mezrioui, “SoK: A Comprehensive Survey on Distributed Ledger Technologies,” in *Proc. IEEE Int. Conf. Blockchain and Cryptocurrency (ICBC)*, pp. 1–16. 2022.
- [17] M. Belotti, N. Božić, G. Pujolle, and S. Secci, “A Vademecum on Blockchain Technologies: When, Which and How,” *IEEE Communications Surveys & Tutorials*. 2019.
- [18] A. Capossele, S. Müller, and A. Penzkofer, “Robustness and Efficiency of Voting Consensus Protocols within Byzantine Infrastructures,” *Blockchain: Research and Applications*, vol. 2, no. 1, Art. no. 100007, doi: 10.1016/j.bcr.2021.100007. 2021.
- [19] A. Carelli, A. Palmieri, A. Vilei, F. Castanier, and A. Vesco, “Enabling Secure Data Exchange through the IOTA Tangle for IoT Constrained Devices,” *Sensors*, vol. 22, no. 4, Art. no. 1384, doi: 10.3390/s22041384. 2022.
- [20] J. Cech, *A Deep Dive Into IOTA*. 2020.
- [21] S. Duan, M. K. Reiter, and H. Zhang, “BEAT: Asynchronous BFT Made Practical,” in *Proc. ACM SIGSAC Conf. Computer and Communications Security (CCS ’18)*, pp. 2028–2041, doi: 10.1145/3243734.3243812. 2018.
- [22] C. Fan, H. Khazaei, Y. Chen, and P. Musilek, “Towards a Scalable DAG-Based Distributed Ledger for Smart Communities,” in *Proc. IEEE 5th World Forum on Internet of Things (WF-IoT)*, pp. 177–182. 2019.
- [23] IOTA Foundation, “IOTA JavaScript API Library,” [Online]. 2018.
- [24] H. Farahani and H. R. Shahriari, “A Privacy Preserving IoT Data Marketplace Using IOTA Smart Contracts.”
- [25] M. Fartitchou, I. Lamaakal, Y. Maleh, K. El Makkaoui, Z. El Allali, P. Pławiak, and F. Alblehai, “IOTASDN: IOTA 2.0 Smart Contracts for Securing SDN Ecosystem,” *Sensors*, vol. 24, no. 17, Art. no. 5716, doi: 10.3390/s24175716. 2024.
- [26] G. G. Gueta, I. Abraham, S. Grossman, D. Malkhi, B. Pinkas, M. K. Reiter, et al., “SBFT: A Scalable and Decentralized Trust Infrastructure,” in *Proc. 49th Annual IEEE/IFIP Int. Conf. Dependable Systems and Networks (DSN)*, pp. 568–580, doi: 10.1109/DSN.2019.00063. 2019.
- [27] M. Jalalmaab, M. Pirani, B. Fidan, and S. Jeon, “Cooperative Estimation of Road Condition Based on Dynamic Consensus and Vehicular Communication,” *IEEE Transactions on Intelligent Vehicles*, vol. 4, no. 1, pp. 90–100. 2019.
- [28] F. Kahmann, F. Honecker, J. Dreyer, M. Fischer, and F. Tönjes, “Performance Comparison of Directed Acyclic Graph-Based Distributed Ledgers and Blockchain Platforms,” *Computers*, vol. 12, no. 12, Art. no. 257, doi: 10.3390/computers12120257. 2023.
- [29] L. Lamport, “Paxos Made Simple,” *ACM SIGACT News*, vol. 32, no. 4, pp. 18–25. 2001.
- [30] B. Lashkari and P. Musilek, “A Comprehensive Review of Blockchain Consensus Mechanisms,” *IEEE Access*, doi: 10.1109/ACCESS.2021.3065880. 2021.

- [31] S. W. Lee and K. B. Sim, "Design and Hardware Implementation of a Simplified DAG-Based Blockchain and New AES-CBC Algorithm for IoT Security," *Electronics*, vol. 10, no. 9, Art. no. 1127. 2021.
- [32] Y. Li, B. Cao, M. Peng, L. Zhang, L. Zhang, D. Feng, and J. Yu, "Directed Acyclic Graph-Based Ledger for Internet of Things: Performance and Security Analysis," *IEEE/ACM Transactions on Networking*, vol. 28, no. 4, pp. 1643–1656, doi: 10.1109/TNET.2020.2991994. 2020.
- [33] B.-Y. Lin, D. Dziubałtowska, P. Macek, A. Penzkofer, and S. Müller, "Robustness of the Tangle 2.0 Consensus," in *Proc. 15th EAI Int. Conf. Performance Evaluation Methodologies and Tools (VALUETOOLS)*, pp. 259–276, doi: 10.1007/978-3-031-31234-2_16. 2023.
- [34] J. Liu, W. Li, G. O. Karame, and N. Asokan, "Scalable Byzantine Consensus via Hardware-Assisted Secret Sharing," *IEEE Transactions on Computers*, vol. 68, no. 1, pp. 139–151, doi: 10.1109/TC.2018.2860009. 2019.
- [35] D. Maliki, C. Oruche, I. M. Abdullahi, B. G. Najashi, O. R. Isah, A. Ahmed, and A. S. Gbadamosi, "An Electronic Voting System with Directed Acyclic Graph (DAG)-Based Blockchain Using ShimmerEVM Network," vol. 1, no. 1. 2024.
- [36] S. Müller, A. Penzkofer, N. Polyanskii, J. Theis, W. Sanders, and H. Moog, "Reality-Based UTXO Ledger," *Distributed Ledger Technologies: Research and Practice*, vol. 2, no. 3, doi: 10.1145/3616022. 2023.
- [37] S. T. Muntaha, Q. Z. Ahmed, F. A. Khan, Z. D. Zaharis, and P. I. Lazaridis, "Hybrid Blockchain-Based Multi-Operator Resource Sharing and SLA Management," *IEEE Open Journal of the Communications Society*, doi: 10.1109/OJCOMS.2024.3523362. 2025.
- [38] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System." 2008.
- [39] P. S. Nzakuna, V. Paciello, A. Lay-Ekuakille, A. K. Lusala, and S. D. Iacono, "Empirical Analysis of the IOTA Tangle Ledger in the Stardust Stage," in *Proc. IEEE Int. Symp. Measurements & Networking (M&N)*, doi: 10.1109/MN60932.2024.10615554. 2024.
- [40] S. Park and H. Kim, "DAG-Based Distributed Ledger for Low-Latency Smart Grid Network," *Energies*, vol. 12, Art. no. 3570, doi: 10.3390/en12183570. 2019. H. Petersen, P. C. Holdgaard, P. H. Madsen, L. M. Knudsen, D. Gad, A. E. Gravergaard, M. Rohde, C. Godballe, B. E. Engelmann, K. Bech, D. Teilmann-Jørgensen, O. Mogensen, J. Karstoft, J. Johansen, J. B. Christensen, A. Johansen, and P. F. Høilund-Carlsen, "FDG PET/CT in Cancer: Comparison of Actual Use with Literature-Based Recommendations," *European Journal of Nuclear Medicine and Molecular Imaging*, vol. 43, pp. 695–706, doi: 10.1007/s00259-015-3217-0. 2016.
- [43] S. Popov, "The Tangle," IOTA Foundation White Paper. 2017.
- [44] S. Popov and W. J. Buchanan, "FPC-BI: Fast Probabilistic Consensus within Byzantine Infrastructures," *Journal of Parallel and Distributed Computing*, vol. 147, pp. 77–86, doi: 10.1016/j.jpdc.2020.09.002. 2021.
- [45] M. Raikwar, N. Polyanskii, and S. Müller, "Fairness Notions in DAG-Based DLTs." 2025.
- [46] T. Ramírez-Gordillo, A. Maciá-Lillo, F. A. Pujol, N. García-D'Urso, J. Azorín-López, and H. Mora, "Decentralized Identity Management for Internet of Things Devices Using IOTA Blockchain Technology," *Future Internet*, vol. 17, no. 1, Art. no. 49. 2025.
- [47] S. Rochman, J. E. Istiyanto, A. Dharmawan, V. Handika, and S. R. Purnama, "Optimization of Tips Selection on the IOTA Tangle for Securing Blockchain-Based IoT Transactions," *Procedia Computer Science*, vol. 216, pp. 230–236. 2023.
- [48] S. Roda, E. Navarro, U. Zdun, V. López-Jaquero, and G. Simhandl, "Past and Future of Software Architectures for Context-Aware Systems: A Systematic Mapping Study," *Journal of Systems and Software*, vol. 146, pp. 310–355. 2018.
- [49] N. Sealey, A. Aijaz, and B. Holden, "IOTA Tangle 2.0: Toward a Scalable, Decentralized, Smart, and Autonomous IoT Ecosystem," in *Proc. Int. Conf. Smart Applications, Communications and Networking (SmartNets)*, pp. 1–8. 2022.

- [50] J. Tian and H. Xu, “TSBFT: A Scalable and Efficient Leaderless Byzantine Consensus for Consortium Blockchain,” *Computer Networks*. 2023.
- [51] M. Vukolić, “The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication,” in *Proc. Int. Workshop Open Problems in Network Security*, pp. 112–125. 2015.
- [52] K. Voulgaridis, D. Karampatzakis, P. Sarigiannidis, and T. Lagkas, “ABS-TD3: Efficient IoT Data Submission in DAG-Based DLTs for Digital Circular Economy,” *Internet of Things*, vol. 34, Art. no. 101814, doi: 10.1016/j.iot.2025.101814. 2025.
- [53] W. Wang, H. D. Thai, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, “A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks,” *IEEE Access*. 2019.
- [54] Q. Wang, J. Yu, S. Chen, and Y. Xiang, “SoK: DAG-Based Blockchain Systems,” *ACM Computing Surveys*, vol. 55, no. 12, doi: 10.1145/3576899. 2023.
- [55] W. M. A. B. Wijesundara, J.-S. Lee, D. Tith, E. Aloupogianni, H. Suzuki, and T. Obi, “Security-Enhanced Firmware Management Scheme for Smart Home IoT Devices Using Distributed Ledger Technologies,” *International Journal of Information Security*, vol. 23, pp. 1927–1937, doi: 10.1007/s10207-024-00827-x. 2024.
- [56] H. Wu, X. Yang, C. Yue, H.-Y. Paik, and S. S. Kanhere, “Chain or DAG? Underlying Data Structures, Architectures, Topologies and Consensus in Distributed Ledger Technology: A Review, Taxonomy and Research Issues,” *Journal of Systems Architecture*, vol. 131, Art. no. 102720, doi: 10.1016/j.sysarc.2022.102720. 2022.
- [57] H. Wu, C. Yue, L. Zhang, Y. Li, and M. A. Imran, “When Distributed Consensus Meets Wireless Connected Autonomous Systems: A Review and a DAG-Based Approach.” 2023.
- [58] Y. Xiao, N. Zhang, J. Li, W. Lou, and Y. T. Hou, “Distributed Consensus Protocols and Algorithms,” in *Blockchain for Distributed Systems Security*. 2019.
- [59] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, “A Survey of Distributed Consensus Protocols for Blockchain Networks,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1432–1465. 2020.
- [60] M. Yin, D. Malkhi, M. K. Reiter, G. G. Gueta, and I. Abraham, “HotStuff: BFT Consensus with Linearity and Responsiveness,” in *Proc. ACM Symp. Principles of Distributed Computing (PODC)*, pp. 347–356. 2019.
- [61] L. Zhao, P. Ferraro, and R. Shorten, “A Smart Mask to Enforce Social Contracts Based on IOTA Tangle,” *PLOS ONE*, doi: 10.1371/journal.pone.0292850. 2024.
- [62] K. Zhang and H.-A. Jacobsen, “Towards Dependable, Scalable, and Pervasive Distributed Ledgers with Blockchains,” in *Proc. IEEE 38th Int. Conf. Distributed Computing Systems (ICDCS)*, pp. 1337–1346. 2018.
- [63] C. Zhang, C. Wu, and X. Wang, “Overview of Blockchain Consensus Mechanism,” in *Proc. 2nd Int. Conf. Big Data Engineering*, pp. 7–12. 2020.
- [64] Y. Zhang, R. Nakanishi, M. A. Sasabe, and S. Kasahara, “Combining IOTA and Attribute-Based Encryption for Access Control in the Internet of Things,” *Sensors*, vol. 21, no. 15, Art. no. 5053, doi: 10.3390/s21155053. 2021.
- [65] S. Zhou, K. Li, L. Xiao, J. Cai, W. Liang, and A. Castiglione, “A Systematic Review of Consensus Mechanisms in Blockchain,” *Mathematics*, vol. 11, Art. no. 2248, doi: 10.3390/math11102248. 2023.

ΠΑΡΑΡΤΗΜΑ Α : ΓΛΩΣΣΑΡΙ ΒΑΣΙΚΩΝ ΟΡΩΝ DLT ΚΑΙ SHIMMER

Τεχνολογία Κατανεμημένου Καθολικού (DLT): Μια αναδυόμενη τεχνολογία που επιτρέπει τον διαμοιρασμό δεδομένων μεταξύ διαφορετικών συμμετεχόντων σε διάφορες τοποθεσίες σε όλο τον κόσμο, δημιουργώντας ένα περιβάλλον χωρίς κεντρικούς διαμεσολαβητές.

Κατευθυνόμενο Ακυκλικό Γράφημα (DAG): Μια δομή δικτύου που, σε αντίθεση με τη γραμμική αλυσίδα του παραδοσιακού blockchain, σχηματίζει ένα κατευθυνόμενο ακυκλικό γράφημα από τα μπλοκ/συναλλαγές, επιτρέποντας την παράλληλη επιβεβαίωσή τους και προσφέροντας υψηλή επεκτασιμότητα.

Tangle: Το πρωτόκολλο και η υποκείμενη δομή δεδομένων —μια συλλογή από κόμβους και βέλη— που χρησιμοποιείται στο οικοσύστημα του IOTA και του Shimmer για την αποθήκευση όλων των συναλλαγών που πραγματοποιούνται μέσω του συστήματος.

Shimmer Network: Ένα πειραματικό δίκτυο σταδιοποίησης (DLT) εντός του οικοσυστήματος του IOTA, το οποίο επιτρέπει την απρόσκοπτη σύνδεση έξυπνων αλυσίδων συμβολαίων και δοκιμάζει νέες τεχνολογίες πριν αυτές εφαρμοστούν στο κύριο δίκτυο.

Μηχανισμός Συναίνεσης (Consensus Mechanism): Η απαραίτητη διαδικασία και το πρωτόκολλο μέσω του οποίου οι συμμετέχοντες κόμβοι σε ένα δυναμικό, αποκεντρωμένο δίκτυο καταλήγουν σε συμφωνία σχετικά με την αυθεντικότητα και την επικύρωση των συναλλαγών.

.