ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πτυχιακή Εργασία

Τίτλος Πτυχιακής Εργασίας	Οι Τεχνολογίες Που Υποστηρίζουν Την Ανάπτυξη Των Κρυπτονομισμάτων Technologies Supporting the Development of Cryptocurrencies
Ονοματεπώνυμο Φοιτητή	Θεοφάνης Κάλιοσης
Πατρώνυμο	Ευάγγελος
Αριθμός Μητρώου	Π20070
Επιβλέπων	Κωνσταντίνος Λιαγκούρας, Επιβλέπων Καθηγητής

Ημερομηνία Παράδοσης **Ιούνιος 2026**

Copyright ©

ΕΥΧΑΡΙΣΤΙΕΣ

Με την ολοκλήρωση της παρούσας πτυχιακής εργασίας, αισθάνομαι την ανάγκη να εκφράσω τις θερμές μου ευχαριστίες προς όλους όσους συνέβαλαν στην εκπόνησή της.

Πρωτίστως, θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου, κ. Κωνσταντίνο Λιαγκούρα, για την εμπιστοσύνη που μου έδειξε αναθέτοντάς μου αυτό το θέμα, καθώς και για την πολύτιμη καθοδήγηση, τις καίριες παρατηρήσεις και τον χρόνο που αφιέρωσε καθ' όλη τη διάρκεια της συνεργασίας μας.

Επίσης, ευχαριστώ τα μέλη της εξεταστικής επιτροπής για τον χρόνο τους και τις εποικοδομητικές τους υποδείξεις.

Τέλος, οφείλω ένα μεγάλο ευχαριστώ στην οικογένειά μου, στους γονείς μου Ευάγγελο Κάλιοση και Στεφανία Ζησάκη και στον αδερφό μου Παναγιώτη Κάλιοση, για την ηθική και υλική στήριξη που μου παρείχαν σε όλη τη διάρκεια των σπουδών μου. Ιδιαίτερες ευχαριστίες ανήκουν στη σύντροφό μου, Έλενα Τόλη, για την υπομονή, την κατανόηση και την αμέριστη συμπαράστασή της σε όλη τη διάρκεια αυτής της προσπάθειας.

Περίληψη

Η παρούσα πτυχιακή εργασία διερευνά την τεχνολογική εξέλιξη, την αρχιτεκτονική δομή και τις κοινωνικοοικονομικές επιπτώσεις της τεχνολογίας Blockchain, από την εμφάνιση του Bitcoin το 2008 έως τις σύγχρονες εφαρμογές του Web3. Στόχος της μελέτης είναι να αναλύσει πώς τα Κατανεμημένα Καθολικά (DLT) μετασχηματίζονται από πειραματικά συστήματα πληρωμών σε μια παγκόσμια υποδομή διακανονισμού αξίας.

Αρχικά, εξετάζεται το θεωρητικό υπόβαθρο, συμπεριλαμβανομένων των κρυπτογραφικών αλγορίθμων (Hashing, Ψηφιακές Υπογραφές) και της δομής δεδομένων (Merkle Trees), ενώ αναλύεται η κρίσιμη μετάβαση από τον ενεργοβόρο μηχανισμό Proof-of-Work (PoW) στο βιώσιμο Proof-of-Stake (PoS). Στη συνέχεια, η εργασία εστιάζει στην επίλυση του "Τριλήμματος της Επεκτασιμότητας" μέσω Αρθρωτών Αρχιτεκτονικών και λύσεων Layer 2 (Rollups), καθώς και στη λειτουργία των Έξυπνων Συμβολαίων που θεμελιώνουν την Αποκεντρωμένη Χρηματοδότηση (DeFi).

Ιδιαίτερη έμφαση δίνεται στη σύγκλιση της τεχνολογίας με την πραγματική οικονομία, μέσω της Τοκενοποίησης Πραγματικών Περιουσιακών Στοιχείων (RWA), των Αποκεντρωμένων Δικτύων Φυσικών Υποδομών (DePIN) και της Αυτοκυρίαρχης Ταυτότητας (SSI), υπό το πρίσμα του νέου κανονιστικού πλαισίου MiCA. Τέλος, αξιολογούνται οι μελλοντικές τάσεις, όπως η θωράκιση έναντι των κβαντικών υπολογιστών και η συνέργεια με την Τεχνητή Νοημοσύνη (Agentic Economy). Το κεντρικό συμπέρασμα είναι ότι η τεχνολογική ωρίμανση του Blockchain σηματοδοτεί τη μετάβαση από το "Διαδίκτυο της Πληροφορίας" στο "Διαδίκτυο της Αξίας", επαναπροσδιορίζοντας την έννοια της ψηφιακής ιδιοκτησίας και εμπιστοσύνης.

Λέξεις-Κλειδιά: Blockchain, DLT, Ethereum, DeFi, Layer 2, RWA, DePIN, Tokenization, Κρυπτογραφία, Web3.

Abstract

This thesis explores the technological evolution, architectural structure, and socioeconomic impact of Blockchain technology, from the inception of Bitcoin in 2008 to modern Web3 applications. The study aims to analyze how Distributed Ledger Technologies (DLT) are transforming from experimental payment systems into a global infrastructure for value settlement.

Initially, the theoretical background is examined, including cryptographic algorithms (Hashing, Digital Signatures) and data structures (Merkle Trees), while analyzing the critical transition from the energy-intensive Proof-of-Work (PoW) to the sustainable Proof-of-Stake (PoS) mechanism. Subsequently, the thesis focuses on solving the "Scalability Trilemma" through Modular Architectures and Layer 2 solutions (Rollups), as well as the function of Smart Contracts that underpin Decentralized Finance (DeFi).

Particular emphasis is placed on the convergence of technology with the real economy through Real World Asset (RWA) tokenization, Decentralized Physical Infrastructure Networks (DePIN), and Self-Sovereign Identity (SSI), within the context of the new MiCA regulatory framework. Finally, future trends are evaluated, such as post-quantum cryptography and synergy with Artificial Intelligence (Agentic Economy). The central conclusion is that the technological maturity of Blockchain signals the transition from the "Internet of Information" to the "Internet of Value," redefining the concepts of digital ownership and trust.

Keywords: Blockchain, DLT, Ethereum, DeFi, Layer 2, RWA, DePIN, Tokenization, Cryptography, Web3.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Κατάλογος Εικόνων

Κατάλογος Πινάκων

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

1.1 Γενικό Πλαίσιο και Επιστημονική Σημασία

Η είσοδος στην τρίτη δεκαετία του 21ου αιώνα σηματοδοτείται από τον ψηφιακό μετασχηματισμό των χρηματοπιστωτικών συστημάτων και την ανάδυση του Web 3.0. Σε αυτό το εξελισσόμενο τοπίο, τα κρυπτονομίσματα (cryptocurrencies) και οι υποκείμενες τεχνολογίες τους δεν αποτελούν πλέον πειραματικές εφαρμογές, αλλά θεμελιώδεις πυλώνες της νέας ψηφιακής οικονομίας. Σύμφωνα με πρόσφατες μελέτες των Hassan et al. (2020), η τεχνολογία του Blockchain έχει υπερβεί τον αρχικό της σκοπό ως μέσο συναλλαγών και έχει εξελιχθεί σε μια πλατφόρμα εμπιστοσύνης (trust machine) που επηρεάζει τομείς όπως η εφοδιαστική αλυσίδα, η υγεία και το Διαδίκτυο των Πραγμάτων (IoT) [1].

Η επιστημονική σημασία της μελέτης των τεχνολογιών που υποστηρίζουν τα κρυπτονομίσματα έγκειται στην ικανότητά τους να επιλύουν μακροχρόνια προβλήματα της πληροφορικής, όπως η επίτευξη συναίνεσης σε κατανεμημένα δίκτυα χωρίς κεντρική αρχή. Όπως επισημαίνουν οι Casino et al. (2020), η μετάβαση από τα κεντρικοποιημένα στα αποκεντρωμένα συστήματα επαναπροσδιορίζει τις έννοιες της ασφάλειας, της ιδιωτικότητας και της διακυβέρνησης δεδομένων [2]. Η παρούσα εργασία εστιάζει στην τεχνική αποδόμηση αυτών των συστημάτων, αναλύοντας τα συστατικά στοιχεία που επιτρέπουν την ασφαλή και αδιάβλητη λειτουργία τους σε ένα εχθρικό περιβάλλον (adversarial environment).

1.2 Ιστορική Εξέλιξη και Τεχνολογικές Γενιές

Η ιστορία των κρυπτονομισμάτων δεν είναι μια απλή γραμμική αφήγηση, αλλά μια διαδικασία τεχνολογικής ωρίμανσης που διακρίνεται σε σαφείς γενιές. Η σύγχρονη βιβλιογραφία (2020-2024) κατηγοριοποιεί αυτή την εξέλιξη σε τρεις φάσεις, ανάλογα με τις δυνατότητες και τους περιορισμούς των πρωτοκόλλων.

1.2.1 Blockchain 1.0: Η Εποχή του Ψηφιακού Νομίσματος Η πρώτη γενιά εστιάζει αποκλειστικά στη λειτουργία της μεταφοράς αξίας και των πληρωμών. Το Bitcoin (BTC), ως ο κύριος εκπρόσωπος, εισήγαγε την έννοια του κατανεμημένου καθολικού (DLT) για την επίλυση του προβλήματος της διπλής δαπάνης (double-spending problem). Οι Gai et al. (2020) αναλύουν πώς αυτή η γενιά έθεσε τα θεμέλια της κρυπτογραφικής ασφάλειας μέσω του αλγορίθμου Proof of Work (PoW) [3]. Πέραν του Bitcoin, σε αυτή τη γενιά ανήκουν και τα πρώτα "altcoins" που προέκυψαν ως παραλλαγές του κώδικά του. Χαρακτηριστικό παράδειγμα είναι το Litecoin (LTC), το οποίο δημιουργήθηκε για να προσφέρει ταχύτερους χρόνους επιβεβαίωσης μπλοκ (2.5 λεπτά έναντι 10 λεπτών του Bitcoin) και διαφορετικό αλγόριθμο hashing (Scrypt). Παρόλα αυτά, η λειτουργικότητα της πρώτης γενιάς παρέμεινε περιορισμένη: δεν υπήρχε η δυνατότητα εκτέλεσης πολύπλοκων εντολών, καθιστώντας τα νομίσματα αυτά ακατάλληλα για την ανάπτυξη εφαρμογών.

1.2.2 Blockchain 2.0: Έξυπνα Συμβόλαια και Προγραμματισιμότητα Η εμφάνιση του Ethereum (ETH) το 2015 σηματοδότησε τη μετάβαση στη δεύτερη γενιά, όπου το Blockchain μετατρέπεται από απλό λογιστικό βιβλίο σε έναν "παγκόσμιο υπολογιστή". Η καινοτομία των Έξυπνων Συμβολαίων (Smart Contracts) επέτρεψε την εκτέλεση αυτοματοποιημένου κώδικα "Turing-complete". Σύμφωνα με τους Wang et al. (2021), αυτή η εξέλιξη άνοιξε τον δρόμο για την Αποκεντρωμένη Οικονομία (DeFi) και τα Non-Fungible Tokens (NFTs), μετατρέποντας τα

κρυπτονομίσματα από απλά tokens σε λειτουργικά στοιχεία λογισμικού [4]. Εκτός από το Ethereum, σημαντικό ρόλο σε αυτή τη γενιά διαδραμάτισαν πλατφόρμες όπως το NEO (συχνά αποκαλούμενο ως το "Κινεζικό Ethereum") και το EOS, τα οποία προσπάθησαν να βελτιώσουν την ταχύτητα συναλλαγών χρησιμοποιώντας διαφορετικούς μηχανισμούς συναίνεσης (Delegated Proof of Stake). Ωστόσο, η δεύτερη γενιά αντιμετώπισε σοβαρά προβλήματα συμφόρησης δικτύου (network congestion) και υψηλών τελών συναλλαγής (gas fees).

1.2.3 Blockchain 3.0 και 4.0: Επεκτασιμότητα και Διαλειτουργικότητα Η τρέχουσα ερευνητική αιχμή, όπως περιγράφεται από τους Zhou et al. (2021), αφορά την τρίτη γενιά που στοχεύει στην επίλυση του "Τριλήμματος του Blockchain" (Scalability Trilemma). Στόχος είναι η δημιουργία δικτύων που είναι ταυτόχρονα ασφαλή, αποκεντρωμένα και γρήγορα [5]. Σε αυτή την κατηγορία εντάσσονται:

- Το Solana (SOL), που εισήγαγε τον καινοτόμο μηχανισμό Proof of History (PoH) για να επιτύχει δεκάδες χιλιάδες συναλλαγές ανά δευτερόλεπτο.
- Το Polkadot (DOT) και το Cosmos (ATOM), τα οποία εστιάζουν στη "Διαλειτουργικότητα" (Interoperability), επιτρέποντας σε διαφορετικά blockchains να επικοινωνούν μεταξύ τους και να ανταλλάσσουν δεδομένα χωρίς κεντρικούς διαμεσολαβητές.
- Το Cardano (ADA), το οποίο αναπτύχθηκε με βάση μια αυστηρή ακαδημαϊκή προσέγγιση και peer-reviewed έρευνα, στοχεύοντας στη βιωσιμότητα και την ασφάλεια των έξυπνων συμβολαίων.

1.3 Ορισμός του Προβλήματος

Η θεμελιώδης πρόκληση που καλούνται να αντιμετωπίσουν οι τεχνολογίες των κρυπτονομισμάτων είναι η δημιουργία εμπιστοσύνης σε ένα περιβάλλον μηδενικής εμπιστοσύνης (trustless environment). Ωστόσο, το πρόβλημα δεν είναι μόνο τεχνικό, αλλά και βαθιά οικονομικό και κοινωνικό.

1.3.1 Τεχνικές Προκλήσεις: Ασφάλεια και Ιδιωτικότητα Τα παραδοσιακά συστήματα βασίζονται σε έναν κεντρικό διαμεσολαβητή (Τράπεζα), ο οποίος αποτελεί μοναδικό σημείο αποτυχίας (Single Point of Failure - SPoF). Οι Li et al. (2021), σε μια εκτενή ανασκόπηση των προκλήσεων ασφαλείας, εντοπίζουν τα εξής κρίσιμα ζητήματα:

1. Ακεραιότητα Δεδομένων: Πώς διασφαλίζεται ότι το ιστορικό συναλλαγών δεν μπορεί να παραποιηθεί αναδρομικά;
2. Ανθεκτικότητα σε Επιθέσεις: Πώς προστατεύεται το δίκτυο από επιθέσεις Sybil (όπου ένας χρήστης δημιουργεί ψεύτικες ταυτότητες) ή επιθέσεις 51%, όπου μια ομάδα αποκτά τον έλεγχο του δικτύου;
3. Ιδιωτικότητα: Πώς διασφαλίζεται η ανωνυμία των χρηστών ενώ ταυτόχρονα το καθολικό είναι δημόσιο; [6].

1.3.2 Οικονομικές και Κοινωνικές Προκλήσεις: Πέρα από την τεχνολογία, τα κρυπτονομίσματα καλούνται να δώσουν λύσεις σε δομικά προβλήματα του παγκόσμιου χρηματοπιστωτικού συστήματος. Σύμφωνα με πρόσφατες μελέτες των Hassan et al. (2020) και άλλων ερευνητών, τα κυριότερα οικονομικά προβλήματα που αντιμετωπίζονται είναι:

- Προστασία από τον Πληθωρισμό: Τα παραδοσιακά νομίσματα (fiat money) υπόκεινται σε πληθωριστικές πιέσεις λόγω της αλόγιστης εκτύπωσης χρήματος από τις κεντρικές τράπεζες. Κρυπτονομίσματα όπως το Bitcoin, με το σταθερό όριο προσφοράς τους (21 εκατομμύρια μονάδες), λειτουργούν ως "ψηφιακός χρυσός" και μέσο διαφύλαξης αξίας (store of value) [1].
- Χρηματοοικονομική Συμπερίληψη (Financial Inclusion): Περίπου 1.7 δισεκατομμύρια άνθρωποι παγκοσμίως παραμένουν "unbanked" (χωρίς τραπεζικό λογαριασμό). Η τεχνολογία blockchain επιτρέπει σε οποιονδήποτε διαθέτει ένα smartphone να αποκτήσει πρόσβαση σε τραπεζικές υπηρεσίες χωρίς γραφειοκρατικά εμπόδια.
- Διασυνοριακές Πληρωμές και Εμβάσματα: Τα τρέχοντα συστήματα (όπως το SWIFT) είναι αργά και ακριβά, ιδιαίτερα για μικρά ποσά. Τα κρυπτονομίσματα επιτρέπουν την άμεση και φθηνή μεταφορά αξίας σε ολόκληρο τον πλανήτη, παρακάμπτοντας τους ενδιάμεσους χρηματοπιστωτικούς οργανισμούς.

1.4 Σκοπός και Στόχοι της Εργασίας

Ο κύριος σκοπός της παρούσας πτυχιακής εργασίας είναι η συστηματική ανάλυση και κριτική αξιολόγηση των τεχνολογικών υποδομών που καθιστούν εφικτή τη λειτουργία των σύγχρονων κρυπτονομισμάτων. Δεν αρκείται σε μια περιγραφική παρουσίαση, αλλά επιδιώκει να συγκρίνει τις διαφορετικές τεχνολογικές προσεγγίσεις που έχουν προταθεί στη βιβλιογραφία της τελευταίας πενταετίας.

Αναλυτικότερα, οι επιμέρους ερευνητικοί στόχοι είναι:

- Στόχος 1: Η εις βάθος ανάλυση της αρχιτεκτονικής των Κατανεμημένων Καθολικών (DLT) και των δομών δεδομένων (Merkle Trees, Directed Acyclic Graphs - DAG) που χρησιμοποιούνται για την αποθήκευση πληροφορίας.
- Στόχος 2: Η συγκριτική μελέτη των Μηχανισμών Συναίνεσης (Consensus Algorithms). Θα εξεταστεί η μετάβαση από ενεργοβόρους αλγορίθμους (PoW) σε πιο βιώσιμες λύσεις (PoS, PoH), όπως αναλύεται από τους Xiao et al. (2020) [7].
- Στόχος 3: Η διερεύνηση των κρυπτογραφικών μεθόδων αιχμής, συμπεριλαμβανομένων των Zero-Knowledge Proofs (ZKPs) και των υπογραφών πολλαπλών μερών (Multi-Sig), που ενισχύουν την ασφάλεια και την ιδιωτικότητα.
- Στόχος 4: Η αξιολόγηση των λύσεων επεκτασιμότητας (Scalability), με έμφαση στα πρωτόκολλα Layer 2 και τις γέφυρες διαλειτουργικότητας (Cross-chain bridges), που αποτελούν το επίκεντρο της τρέχουσας έρευνας.

1.5 Μεθοδολογική Προσέγγιση

Η εκπόνηση της εργασίας βασίζεται στη μεθοδολογία της συστηματικής βιβλιογραφικής ανασκόπησης (Systematic Literature Review - SLR). Σύμφωνα με τις οδηγίες του Τμήματος Πληροφορικής του Πανεπιστημίου Πειραιώς, η αναζήτηση πηγών περιορίστηκε σε επιστημονικά άρθρα δημοσιευμένα την περίοδο 2020-2025. Χρησιμοποιήθηκαν βάσεις δεδομένων υψηλού

κύρους, όπως το ScienceDirect, το IEEE Xplore και το SpringerLink, με κριτήριο την κατάταξη των περιοδικών (Q1/Q2 βάσει Scimago). Η επιλογή των άρθρων έγινε με βάση τη συνάφειά τους με τις λέξεις-κλειδιά: "Blockchain architecture", "Consensus protocols survey", "Cryptocurrency security", και "Smart contracts evolution".

1.6 Δομή της Εργασίας

Η παρούσα μελέτη διαρθρώνεται σε εννέα διακριτά κεφάλαια, τα οποία ακολουθούν μια λογική αλληλουχία από τη θεωρία στην πράξη και από το θεμελιώδες στο σύνθετο.

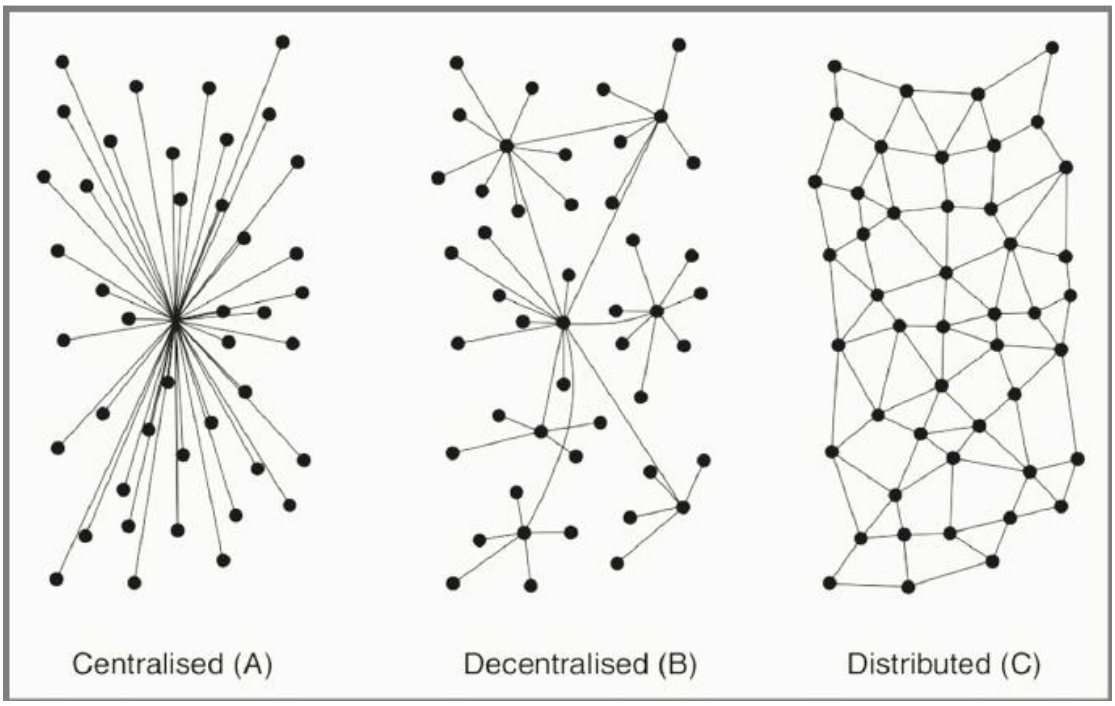
- Στο Κεφάλαιο 2, παρουσιάζεται αναλυτικά η μεθοδολογία έρευνας που ακολουθήθηκε.
- Το Κεφάλαιο 3 εστιάζει στην Αρχιτεκτονική των Συστημάτων DLT, αναλύοντας τη δομή των μπλοκ και τα δίκτυα P2P.
- Το Κεφάλαιο 4 εξετάζει το υπόβαθρο της Κρυπτογραφίας (Hashing, Ασύμμετρη Κρυπτογραφία), καθώς και προηγμένες τεχνικές διασφάλισης της ιδιωτικότητας.
- Το Κεφάλαιο 5 αποτελεί τον πυρήνα της ανάλυσης των Μηχανισμών Συναίνεσης (PoW vs PoS).
- Το Κεφάλαιο 6 εισάγει την έννοια των Έξυπνων Συμβολαίων, τις αποκεντρωμένες εφαρμογές (dApps) και τις προκλήσεις ασφαλείας αυτών.
- Το Κεφάλαιο 7 αναλύει το Τρίλημμα της Επεκτασιμότητας, τις σύγχρονες λύσεις Δεύτερου Επιπέδου (Layer 2) και τους μηχανισμούς Διαλειτουργικότητας μεταξύ ανεξάρτητων δικτύων (Bridges, Cosmos, Polkadot).
- Το Κεφάλαιο 8 επικεντρώνεται στις Εφαρμογές του Blockchain στον Πραγματικό Κόσμο (όπως RWA, CBDCs, SSI, DePIN) και στο σύγχρονο ρυθμιστικό πλαίσιο (π.χ. κανονισμός MiCA).
- Τέλος, στο Κεφάλαιο 9, παρατίθενται τα τελικά συμπεράσματα της μελέτης και διατυπώνονται προτάσεις για μελλοντική έρευνα.

ΚΕΦΑΛΑΙΟ 2: ΘΕΩΡΗΤΙΚΟ ΥΠΟΒΑΘΡΟ ΚΑΙ ΔΟΜΗ ΤΟΥ BLOCKCHAIN

2.1 Από τα Κατανεμημένα Καθολικά (DLT) στο Blockchain

Η τεχνολογία Blockchain συχνά συγχέεται με τον ευρύτερο όρο Distributed Ledger Technology (DLT) ή Τεχνολογία Κατανεμημένου Καθολικού. Ωστόσο, στην ακαδημαϊκή βιβλιογραφία, η σχέση τους είναι ιεραρχική: όλα τα Blockchains είναι DLTs, αλλά δεν είναι όλα τα DLTs Blockchains.

Σύμφωνα με τους Wegrzyn & Wang (2021), η DLT ορίζεται ως μια βάση δεδομένων που είναι διαμοιρασμένη (replicated), συγχρονισμένη (synchronized) και προσβάσιμη από ένα δίκτυο κόμβων που βρίσκονται σε διαφορετικές γεωγραφικές τοποθεσίες, χωρίς την ανάγκη κεντρικού διαχειριστή ή ενδιάμεσου [16]. Η καινοτομία του Blockchain έγκειται στον συγκεκριμένο τρόπο δομής των δεδομένων (σε αλυσίδα μπλοκ), ενώ άλλες μορφές DLT μπορεί να χρησιμοποιούν διαφορετικές δομές.



Εικόνα 2.1: Διαγραμματική απεικόνιση Κεντρικοποιημένων, Αποκεντρωμένων και Κατανεμημένων Δικτύων

2.1.1 Το Πρόβλημα των Βυζαντινών Στρατηγών: Η θεμελιώδης πρόκληση που καλείται να επιλύσει κάθε σύστημα DLT είναι η επίτευξη ομοφωνίας (Consensus) σε ένα περιβάλλον όπου οι συμμετέχοντες δεν εμπιστεύονται ο ένας τον άλλον. Αυτό το πρόβλημα διατυπώθηκε μαθηματικά από τους Lamport, Shostak και Pease (1982) ως το "Πρόβλημα των Βυζαντινών Στρατηγών" [18].

- Το Θεωρητικό Πλαίσιο: Φανταστείτε στρατηγούς που πολιορκούν μια πόλη και επικοινωνούν μόνο με αγγελιοφόρους. Πρέπει να συμφωνήσουν σε κοινή στρατηγική (Επίθεση ή Υποχώρηση). Αν ορισμένοι στρατηγοί είναι προδότες (κακόβουλοι κόμβοι) και στείλουν αντικρουόμενα μηνύματα, η επίθεση θα αποτύχει.
- Η Λύση του Nakamoto: Το Bitcoin έλυσε αυτό το πρόβλημα πιθανοτικά, εισάγοντας τον μηχανισμό Proof-of-Work. Οι "τίμιοι" κόμβοι αποδεικνύουν την αλήθεια ξοδεύοντας ενέργεια (CPU power), καθιστώντας την "προδοσία" (επίθεση στο δίκτυο) οικονομικά ασύμφορη [8].

2.1.2 Θεωρητικά Όρια: Το Θεώρημα CAP Στον σχεδιασμό κατανεμημένων συστημάτων, ισχύει το Θεώρημα CAP (γνωστό και ως Brewer’s Theorem), το οποίο διατυπώθηκε από τον Eric Brewer (2000). Σύμφωνα με αυτό, ένα κατανεμημένο σύστημα μπορεί να εγγυηθεί ταυτόχρονα μόνο δύο από τις εξής τρεις ιδιότητες [95]:

1. Συνέπεια (Consistency): Όλοι οι κόμβοι βλέπουν τα ίδια δεδομένα την ίδια ακριβώς χρονική στιγμή.
2. Διαθεσιμότητα (Availability): Κάθε αίτημα λαμβάνει απάντηση (επιτυχία/αποτυχία), χωρίς εγγύηση ότι τα δεδομένα είναι τα πιο πρόσφατα.

3. Ανεκτικότητα σε Διαμερισμό (Partition Tolerance): Το σύστημα συνεχίζει να λειτουργεί ακόμα και αν διακοπεί η επικοινωνία μεταξύ ομάδων κόμβων.

Τα δημόσια Blockchains (όπως το Bitcoin και το Ethereum) θυσιάζουν την άμεση *Συνέπεια* για να εξασφαλίσουν *Διαθεσιμότητα* και *Ανεκτικότητα σε Διαμερισμό* (AP systems). Γι' αυτόν τον λόγο υπάρχει η έννοια των "confirmations" (επιβεβαιώσεων): δεν είμαστε σίγουροι για την κατάσταση του καθολικού αμέσως (Consistency), αλλά αποκτούμε βεβαιότητα με την πάροδο του χρόνου (Eventual Consistency).

2.1.3 Δομικές Διαφορές: Blockchain vs. Generic DLT Η βασική διαφορά έγκειται στη δομή αποθήκευσης:

- Blockchain: Τα δεδομένα ομαδοποιούνται σε μπλοκ, τα οποία συνδέονται γραμμικά και χρονολογικά χρησιμοποιώντας κρυπτογραφικούς δείκτες (hashes). Κάθε νέο μπλοκ ενισχύει την ασφάλεια των προηγούμενων [11].
- Generic DLT: Μπορεί να μην χρησιμοποιεί μπλοκ. Οι συναλλαγές μπορεί να αποθηκεύονται ανεξάρτητα ή σε άλλες δομές. Παράδειγμα αποτελεί το R3 Corda, όπου οι συναλλαγές είναι ορατές μόνο στα συμβαλλόμενα μέρη για λόγους τραπεζικού απορρήτου, και όχι σε όλο το δίκτυο.

2.1.4 Εναλλακτική Αρχιτεκτονική: Directed Acyclic Graphs (DAG) Μια σημαντική κατηγορία DLT που *δεν* είναι Blockchain είναι οι Κατευθυνόμενοι Ακυκλικοί Γράφοι (DAG). Χρησιμοποιούνται από κρυπτονομίσματα όπως το IOTA (Tangle). Σύμφωνα με τον Popov (2018), σε ένα σύστημα DAG δεν υπάρχουν μπλοκ και miners. Κάθε χρήστης που εκδίδει μια νέα συναλλαγή πρέπει να επαληθεύσει δύο προηγούμενες συναλλαγές. Αυτό δημιουργεί μια δομή πλέγματος (mesh) αντί για αλυσίδα [96].

- Πλεονέκτημα: Θεωρητικά άπειρη επεκτασιμότητα, καθώς όσο περισσότεροι χρήστες μπαίνουν, τόσο πιο γρήγορο γίνεται το δίκτυο.
- Μειονέκτημα: Δυσκολία στην επίτευξη απόλυτης χρονικής σειράς και οριστικότητας (Finality) χωρίς κεντρικό συντονιστή.

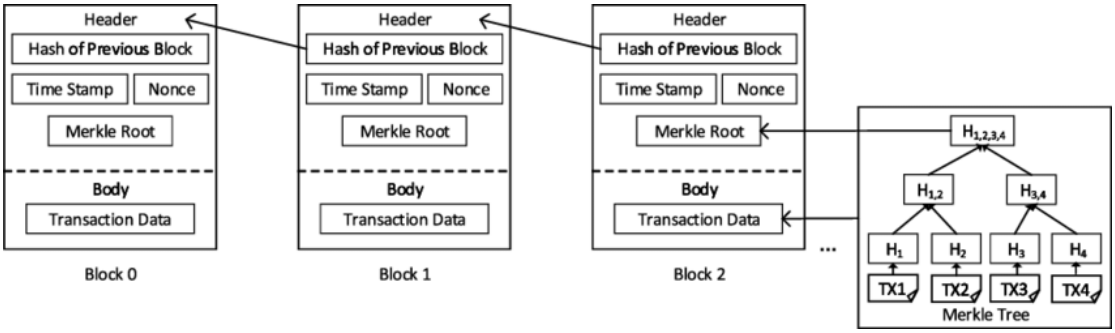
2.1.5 Ταξινόμηση Συστημάτων DLT: Με βάση τα δικαιώματα πρόσβασης και συμμετοχής στη συναίνεση, τα συστήματα διακρίνονται σε τρεις κατηγορίες [16]:

1. Δημόσια (Public / Permissionless): Οποιοσδήποτε μπορεί να συμμετέχει, να διαβάζει και να γράφει δεδομένα (π.χ. Bitcoin, Ethereum). Είναι πλήρως αποκεντρωμένα και ανθεκτικά στη λογοκρισία.
2. Ιδιωτικά (Private / Permissioned): Η πρόσβαση ελέγχεται από έναν κεντρικό οργανισμό. Μόνο εξουσιοδοτημένοι κόμβοι τηρούν το καθολικό. Ένα χαρακτηριστικό παράδειγμα είναι το Hyperledger Fabric, το οποίο χρησιμοποιείται από επιχειρήσεις για ιδιωτικές συναλλαγές υψηλής ταχύτητας [97].
3. Κοινοπραξίας (Consortium / Federated): Η διαδικασία συναίνεσης ελέγχεται από μια προεπιλεγμένη ομάδα κόμβων (π.χ. μια ένωση 15 τραπεζών). Προσφέρει ισορροπία μεταξύ ταχύτητας και αποκέντρωσης.

2.2 Η Ανατομία και η Δομή ενός Μπλοκ (Block Structure)

Στην επιστήμη των υπολογιστών, το Blockchain ορίζεται ως μια μονόδρομη συνδεδεμένη λίστα (singly linked list) μπλοκ. Κάθε μπλοκ είναι ένα ψηφιακό "κ container" που περιέχει μια σειρά από εγγραφές (συναλλαγές). Η θεμελιώδης καινοτομία του Satoshi Nakamoto [8] δεν ήταν η εφεύρεση των μπλοκ, αλλά ο τρόπος σύνδεσής τους: κάθε μπλοκ περιέχει το ψηφιακό αποτύπωμα (Hash) του *προηγούμενου* μπλοκ. Αυτό δημιουργεί μια αλυσίδα εμπιστοσύνης που εκτείνεται μέχρι το πρώτο μπλοκ (Genesis Block).

Ένα τυπικό μπλοκ (με βάση το πρότυπο του Bitcoin) αποτελείται από δύο κύρια μέρη: την Επικεφαλίδα (Block Header) και το Σώμα (Block Body).



Εικόνα 2.2: Ανατομία ενός μπλοκ και κρυπτογραφική σύνδεση με το προηγούμενο μέσω της συνάρτησης κατακερματισμού (Hash).

2.2.1 Η Επικεφαλίδα του Μπλοκ (Block Header): Η επικεφαλίδα είναι το πιο κρίσιμο τμήμα, καθώς είναι αυτό που "εξορύσσεται" (mined) και αυτό που επαληθεύουν οι κόμβοι. Έχει μέγεθος μόλις 80 Bytes και περιλαμβάνει έξι πεδία μεταδεδομένων:

1. Version (4 bytes): Ο αριθμός έκδοσης του λογισμικού (π.χ. Bitcoin Core v0.19). Επιτρέπει στους κόμβους να γνωρίζουν ποιοι κανόνες ισχύουν για το συγκεκριμένο μπλοκ.
2. Previous Block Hash (32 bytes): Αυτός είναι ο "κρίκος" της αλυσίδας. Είναι το SHA-256 hash της επικεφαλίδας του προηγούμενου μπλοκ (Parent Block).
    - *Σημασία για την Ασφάλεια:* Εάν ένας επιτιθέμενος προσπαθήσει να αλλάξει έστω και ένα κόμμα σε μια συναλλαγή του 2015, θα αλλάξει το Merkle Root του μπλοκ του 2015. Αυτό θα αλλάξει το Hash του μπλοκ. Επειδή το επόμενο μπλοκ περιέχει αυτό το Hash, θα ακυρωθεί. Η αλλαγή θα πρέπει να διαδοθεί σε όλα τα επόμενα μπλοκ μέχρι σήμερα, κάτι που απαιτεί απαγορευτική υπολογιστική ισχύ [11].
3. Merkle Root (32 bytes): Ένα hash που αποτελεί τη "σύνοψη" όλων των συναλλαγών που περιέχονται στο σώμα του μπλοκ (βλ. ενότητα 2.3).
4. Timestamp (4 bytes): Η χρονική στιγμή δημιουργίας του μπλοκ σε δευτερόλεπτα από την εποχή UNIX (Unix Epoch). Το δίκτυο απορρίπτει μπλοκ που έχουν χρόνο πολύ μπροστά στο μέλλον ή πολύ πίσω στο παρελθόν.
5. Difficulty Target / nBits (4 bytes): Ένας κωδικοποιημένος αριθμός που ορίζει πόσο δύσκολο είναι να βρεθεί το hash του μπλοκ. Όσο μικρότερος είναι ο στόχος, τόσο πιο δύσκολη η εξόρυξη. Προσαρμόζεται κάθε 2016 μπλοκ (~2 εβδομάδες).
6. Nonce (4 bytes): Ο "Αριθμός που χρησιμοποιείται μία φορά" (Number used ONCE). Είναι η μεταβλητή που αλλάζουν οι miners δισεκατομμύρια φορές το δευτερόλεπτο

προσπαθώντας να λύσουν τον γρίφο του Proof-of-Work, ώστε το τελικό hash να είναι μικρότερο από το Target [8].

2.2.2 Το Σώμα του Μπλοκ (Block Body): Το σώμα καταλαμβάνει τον περισσότερο χώρο (περίπου 1MB - 4MB) και περιέχει τις συναλλαγές.

- Transaction Counter: Πόσες συναλλαγές υπάρχουν στο μπλοκ (π.χ. 2.500).
- Coinbase Transaction: Η πρώτη συναλλαγή σε κάθε μπλοκ είναι ειδική. Δεν προέρχεται από άλλον χρήστη, αλλά δημιουργείται "από το μηδέν" (out of thin air). Είναι η συναλλαγή που πληρώνει τον miner με τα νέα νομίσματα (Block Reward) και τα τέλη συναλλαγών (Transaction Fees).
- Λίστα Συναλλαγών: Οι υπόλοιπες συναλλαγές, επαληθευμένες και υπογεγραμμένες ψηφιακά.

2.2.3 Το Μπλοκ Γένεσης (Genesis Block): Το πρώτο μπλοκ κάθε blockchain (Block 0) ονομάζεται Genesis Block.

- Δεν έχει προηγούμενο hash (είναι όλα μηδενικά).
- Είναι "σκληρά κωδικοποιημένο" (hardcoded) στο λογισμικό και δεν μπορεί να αλλάξει.
- *Ιστορικό Στοιχείο:* Στο Coinbase transaction του Genesis Block του Bitcoin, ο Satoshi Nakamoto έκρυψε το μήνυμα: *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"*. Αυτό αποδεικνύει την ημερομηνία έναρξης και τον πολιτικό σκοπό του Bitcoin ως εναλλακτική στο τραπεζικό σύστημα [11].

2.2.4 Μέγεθος και Βάρος Μπλοκ (Block Size vs Block Weight): Αρχικά, το Bitcoin είχε αυστηρό όριο 1MB ανά μπλοκ για να αποτρέψει επιθέσεις Spam. Καθώς το δίκτυο μεγάλωνε, αυτό δημιούργησε συμφόρηση. Το 2017, με την αναβάθμιση Segregated Witness (SegWit), η έννοια του μεγέθους άλλαξε σε "Βάρος Μπλοκ" (Block Weight).

- Τα δεδομένα χωρίστηκαν σε "Βασικά" (Base data) και "Μάρτυρες" (Witness data - υπογραφές).
- Οι υπογραφές "ζυγίζουν" λιγότερο (0.25 weight units) από τα βασικά δεδομένα (1 weight unit).
- Αυτό επέτρεψε στα μπλοκ να φτάσουν θεωρητικά τα 4MB, αυξάνοντας την χωρητικότητα χωρίς Hard Fork [98].

2.2.5 Αναγνωριστικά Μπλοκ (Block Identifiers): Κάθε μπλοκ έχει δύο ταυτότητες:

1. Block Hash: Το ψηφιακό αποτύπωμα (π.χ. 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f). Είναι μοναδικό αλλά δεν περιέχεται μέσα στο μπλοκ (υπολογίζεται από τους κόμβους).

2. Block Height: Η θέση του στην αλυσίδα (π.χ. Block #830,000). Δεν είναι μοναδικό, καθώς σε περίπτωση διακλάδωσης (Fork), δύο διαφορετικά μπλοκ μπορεί να έχουν το ίδιο ύψος προσωρινά.

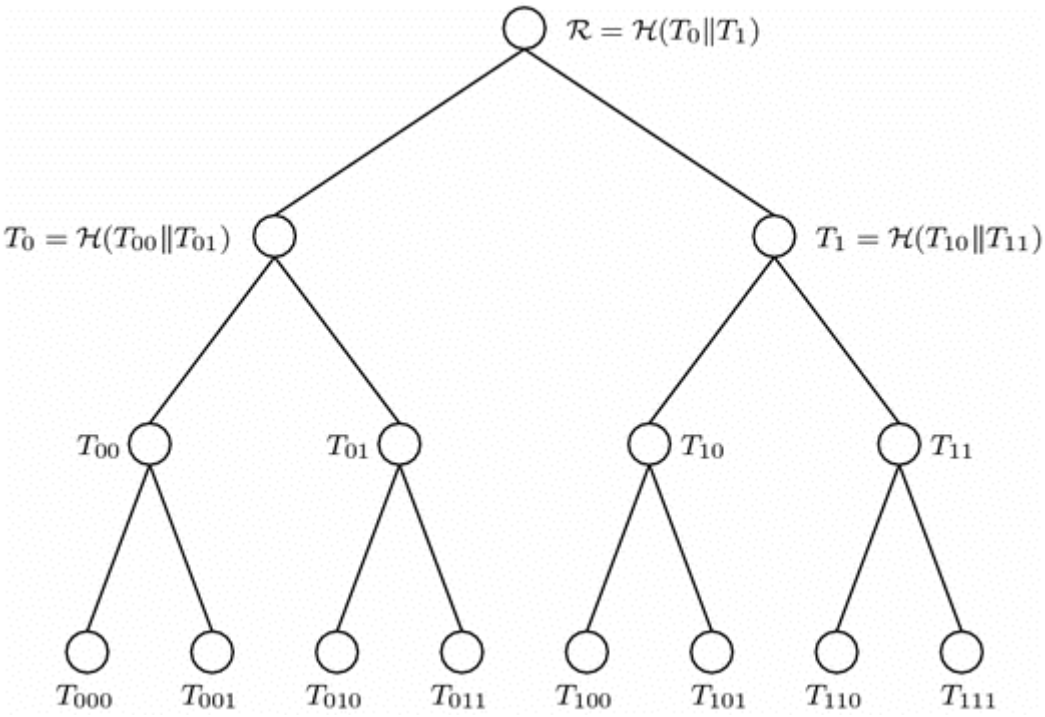
2.3 Δέντρα Merkle (Merkle Trees) και Επαλήθευση Συναλλαγών

Μια από τις μεγαλύτερες προκλήσεις στα κατανεμημένα συστήματα είναι η αποδοτική επαλήθευση της ακεραιότητας των δεδομένων. Σε ένα Blockchain που μεγαλώνει συνεχώς (το Bitcoin ξεπερνά τα 500GB), είναι αδύνατο για κάθε συσκευή (π.χ. smartphone, IoT sensor) να αποθηκεύει όλο το ιστορικό.

Η λύση σε αυτό το πρόβλημα δόθηκε από τον Ralph Merkle (1987) με την εφεύρεση του Δέντρου Merkle (Merkle Tree) ή Δέντρου Κατακερματισμού [27].

2.3.1 Δομή και Λειτουργία: Το Δέντρο Merkle είναι μια δομή δεδομένων τύπου δυαδικού δέντρου (binary tree), όπου κάθε κόμβος είναι το κρυπτογραφικό hash των παιδιών του. Η κατασκευή του γίνεται από κάτω προς τα πάνω (bottom-up approach):

1. Φύλλα (Leaf Nodes): Αρχικά, λαμβάνουμε όλες τις συναλλαγές του μπλοκ και υπολογίζουμε το Hash τους (TXID). Αυτά αποτελούν τη βάση του δέντρου.
2. Γονείς (Parent Nodes): Τα hashes ζευγαρώνονται ανά δύο (H1 με H2, H3 με H4). Κάθε ζεύγος συνενώνεται και περνάει ξανά από τη συνάρτηση hash (π.χ. Hash(H1 + H2) = H12).
3. Ρίζα (Merkle Root): Η διαδικασία επαναλαμβάνεται μέχρι να μείνει μόνο ένα hash στην κορυφή της πυραμίδας. Αυτό ονομάζεται Merkle Root και είναι το μοναδικό στοιχείο που αποθηκεύεται στην Επικεφαλίδα του Μπλοκ (Block Header) [11].



Εικόνα 2.3: Δομή Δέντρου Merkle (Merkle Tree). Οι συναλλαγές κατακερματίζονται και συνδυάζονται ανά ζεύγη μέχρι να παραχθεί η Ρίζα Merkle.

2.3.2 Απλοποιημένη Επαλήθευση Πληρωμών (Simplified Payment Verification - SPV):

Ο Satoshi Nakamoto στο Whitepaper του Bitcoin περιέγραψε τη μέθοδο SPV, η οποία επιτρέπει σε "ελαφρούς κόμβους" (Light Clients) να επαληθεύουν συναλλαγές χωρίς να κατεβάζουν όλο το Blockchain [8].

- Το Πρόβλημα: Έστω ότι η Alice θέλει να αποδείξει στον Bob ότι της έστειλε 1 BTC στη συναλλαγή Tx_K που βρίσκεται στο Μπλοκ #100. Ο Bob έχει κινητό και δεν μπορεί να ελέγξει όλο το μπλοκ (που έχει 2.000 συναλλαγές).
- Η Λύση (Merkle Proof): Η Alice δεν στέλνει στον Bob όλες τις 2.000 συναλλαγές. Του στέλνει μόνο το "Μονοπάτι Merkle" (Merkle Path): τα hashes που χρειάζονται για να φτάσει από τη συναλλαγή Tx_K στη Ρίζα.
- Η Διαδικασία:
    1. Ο Bob παίρνει το Hash της Tx_K.
    2. Το συνδυάζει με το γειτονικό hash που του έδωσε η Alice.
    3. Επαναλαμβάνει τη διαδικασία ανεβαίνοντας το δέντρο.
    4. Αν το τελικό hash που θα βρει ταιριάζει με το Merkle Root που έχει αποθηκευμένο στην επικεφαλίδα του μπλοκ, τότε η συναλλαγή είναι έγκυρη και αμετάβλητη.

2.3.3 Υπολογιστική Πολυπλοκότητα και Αποδοτικότητα

Η δύναμη των Merkle Trees βρίσκεται στα μαθηματικά.

Για να επαληθεύσουμε αν μια συναλλαγή ανήκει σε ένα μπλοκ με N συναλλαγές:

- Χωρίς Merkle Tree: Χρειαζόμαστε $O(N)$ δεδομένα (κατεβάζουμε όλο το μπλοκ).
- Με Merkle Tree: Χρειαζόμαστε $O(\log_2 N)$ δεδομένα (κατεβάζουμε μόνο το κλαδί).

Παράδειγμα:

Σε ένα μπλοκ με 4.000 συναλλαγές (μέγεθος ~4MB):

- Ένας Full Node κατεβάζει 4MB.
- Ένας SPV Node κατεβάζει μόνο την επικεφαλίδα (80 bytes) και ένα Merkle Path περίπου 12 hashes (~384 bytes). Η εξοικονόμηση bandwidth είναι τεράστια [11].

2.3.4 Ιδιωτικότητα και Φίλτρα Bloom (Bloom Filters): Παρόλο που τα SPV πορτοφόλια είναι ελαφριά, έχουν ένα μειονέκτημα ιδιωτικότητας: όταν το πορτοφόλι ζητά από έναν Full Node "δώσε μου τις συναλλαγές για τη διεύθυνση Χ", αποκαλύπτει ποια είναι η διεύθυνσή του.

Για να λυθεί αυτό, χρησιμοποιούνται τα Φίλτρα Bloom. Το πορτοφόλι δεν ζητά συγκεκριμένα δεδομένα, αλλά στέλνει ένα πιθανοτικό φίλτρο (ένα μοτίβο). Ο Full Node απαντά με όλα τα δεδομένα που ταιριάζουν στο μοτίβο. Αυτό περιλαμβάνει τις συναλλαγές του χρήστη, αλλά και άσχετες συναλλαγές ("θόρυβο"), κρύβοντας έτσι το πραγματικό οικονομικό ενδιαφέρον του χρήστη.

2.4 Τυπολογία και Ταξινόμηση Δικτύων Blockchain

Η τεχνολογία Blockchain δεν είναι μονολιθική. Ανάλογα με τους κανόνες συμμετοχής, πρόσβασης και επικύρωσης συναλλαγών, τα δίκτυα κατηγοριοποιούνται σε διαφορετικούς τύπους. Σύμφωνα με τον Vitalik Buterin (2015), η βασική διάκριση έγκειται στο ερώτημα: *"Ποιος έχει το δικαίωμα να γράφει στο καθολικό και ποιος έχει το δικαίωμα να το διαβάζει;"* [99]. Αυτή η ταξινόμηση καθορίζει όχι μόνο την αρχιτεκτονική του δικτύου αλλά και τις περιπτώσεις χρήσης (Use Cases).

2.4.1 Δημόσια / Μη-αδειοδοτημένα Δίκτυα (Public / Permissionless): Είναι η "καθαρή" μορφή του Blockchain, όπως οραματίστηκε από τον Satoshi Nakamoto.

- Πρόσβαση: Ανοιχτή σε όλους (Open Access). Οποιοσδήποτε μπορεί να κατεβάσει το λογισμικό, να τρέξει έναν κόμβο, να στείλει συναλλαγές και να συμμετάσχει στη διαδικασία συναίνεσης (Mining/Staking).
- Ταυτοποίηση: Ανωνυμία ή Ψευδωνυμία. Οι χρήστες δεν χρειάζεται να αποκαλύψουν την ταυτότητά τους (KYC). Αναγνωρίζονται μόνο από τις κρυπτογραφικές τους διευθύνσεις.
- Συναίνεση: Απαιτούνται "βαριοί" μηχανισμοί όπως το Proof-of-Work (PoW) ή το Proof-of-Stake (PoS). Επειδή οι συμμετέχοντες είναι άγνωστοι και δυνητικά κακόβουλοι, το σύστημα πρέπει να κάνει την επίθεση οικονομικά ασύμφορη (μέσω κόστους ενέργειας ή δέσμευσης κεφαλαίου).
- Χαρακτηριστικά:

- *Ανθεκτικότητα στη Λογοκρισία (Censorship Resistance):* Κανείς δεν μπορεί να μπλοκάρει μια συναλλαγή.
- *Αμετάβλητο (Immutability):* Είναι σχεδόν αδύνατο να αλλάξει το ιστορικό.
- *Μειονέκτημα:* Χαμηλή ταχύτητα (TPS) και υψηλή κατανάλωση πόρων.

- Παραδείγματα: Bitcoin, Ethereum, Solana.

2.4.2 Ιδιωτικά / Αδειοδοτημένα Δίκτυα (Private / Permissioned): Αυτά τα δίκτυα λειτουργούν περισσότερο ως κατανεμημένες βάσεις δεδομένων για επιχειρηματική χρήση.

- Πρόσβαση: Ελεγχόμενη. Ένας κεντρικός οργανισμός (π.χ. μια εταιρεία) αποφασίζει ποιος μπορεί να γίνει κόμβος. Η ανάγνωση των δεδομένων μπορεί να είναι δημόσια ή περιορισμένη.
- Ταυτοποίηση: Γνωστή Ταυτότητα. Όλοι οι κόμβοι είναι πιστοποιημένοι και γνωστοί. Χρησιμοποιούνται ψηφιακά πιστοποιητικά (X.509 Certificates) για την ταυτοποίηση.
- Συναίνεση: Ελαφριοί μηχανισμοί. Επειδή οι κόμβοι είναι γνωστοί και εμπιστευόμαστε ότι δεν θα επιτεθούν στο δίκτυο, χρησιμοποιούνται αλγόριθμοι όπως το RAFT ή το PBFT (Practical Byzantine Fault Tolerance). Δεν χρειάζεται εξόρυξη, άρα η ταχύτητα είναι τεράστια (>20.000 TPS) [97].
- Χαρακτηριστικά:
  - *Ιδιωτικότητα:* Τα δεδομένα δεν είναι ορατά στους ανταγωνιστές.
  - *Απόδοση:* Υψηλή ταχύτητα, μηδενικό κόστος συναλλαγής.
  - *Μειονέκτημα:* Είναι κεντρικοποιημένα. Ο διαχειριστής μπορεί να αλλάξει τους κανόνες ή να διαγράψει συναλλαγές.
- Παραδείγματα: Hyperledger Fabric (IBM), Quorum (JPMorgan).

2.4.3 Δίκτυα Κοινοπραξίας (Consortium / Federated Blockchains): Αποτελούν τη "χρυσή τομή" μεταξύ Δημόσιων και Ιδιωτικών.

- Δομή: Το δίκτυο δεν ελέγχεται από έναν οργανισμό, αλλά από μια ομάδα οργανισμών (Consortium).
- Συναίνεση: Η εγκυρότητα ενός μπλοκ απαιτεί την υπογραφή της πλειοψηφίας των μελών (π.χ. 10 από τις 15 τράπεζες). Αυτό ονομάζεται Federated Byzantine Agreement (FBA) [100].
- Περίπτωση Χρήσης: Τραπεζικός τομέας. Οι τράπεζες θέλουν γρήγορες συναλλαγές μεταξύ τους, δεν θέλουν τα δεδομένα τους να είναι δημόσια στο Ethereum, αλλά δεν εμπιστεύονται και η μία την άλλη για να δώσουν τον απόλυτο έλεγχο σε μία τράπεζα. Το Consortium λύνει αυτό το πρόβλημα.
- Παραδείγματα: R3 Corda, Energy Web Chain, Libra (Diem).

2.4.4 Υβριδικά Δίκτυα (Hybrid Blockchains): Μια νεότερη προσέγγιση που συνδυάζει τα πλεονεκτήματα και των δύο κόσμων.

- Λειτουργία: Τα δεδομένα αποθηκεύονται σε ιδιωτική αλυσίδα (για ταχύτητα και ιδιωτικότητα), αλλά το Hash του κάθε μπλοκ ("άγκυρα") αποθηκεύεται περιοδικά σε μια δημόσια αλυσίδα (π.χ. Ethereum) για αμετάβλητοτητα.
- Οφέλη: Η επιχείρηση κρατά τα δεδομένα της κρυφά, αλλά μπορεί να αποδείξει στο κοινό ότι δεν τα έχει παραποιήσει, δείχνοντας το hash στο Public Blockchain.
- Παραδείγματα: Dragonchain, XinFin.

2.4.5 Συγκριτική Ανάλυση: Η επιλογή του κατάλληλου τύπου εξαρτάται από τις ανάγκες της εφαρμογής.

ΚΕΦΑΛΑΙΟ 3: ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑ ΚΑΤΑΝΕΜΗΜΕΝΟΥ ΚΑΘΟΛΙΚΟΥ (DLT)

3.1 Εισαγωγή στα Κατανεμημένα Συστήματα και το DLT

Η τεχνολογία Blockchain δεν αποτελεί παρθενογένεση, αλλά την εξέλιξη των Κατανεμημένων Συστημάτων (Distributed Systems) που μελετώνται στην επιστήμη της πληροφορικής εδώ και δεκαετίες. Εντάσσεται στην ευρύτερη οικογένεια των Τεχνολογιών Κατανεμημένου Καθολικού (Distributed Ledger Technologies - DLT). Σύμφωνα με τους Hassan et al. (2020), η βασική διαφορά του Blockchain από τις παραδοσιακές κατανεμημένες βάσεις δεδομένων (όπως οι NoSQL databases) έγκειται στο ότι λειτουργεί σε "εχθρικό περιβάλλον" (adversarial environment). Οι κόμβοι του δικτύου δεν εμπιστεύονται ο ένας τον άλλον και δεν υπάρχει κεντρική αρχή να επιλύσει τις διαφορές [8].

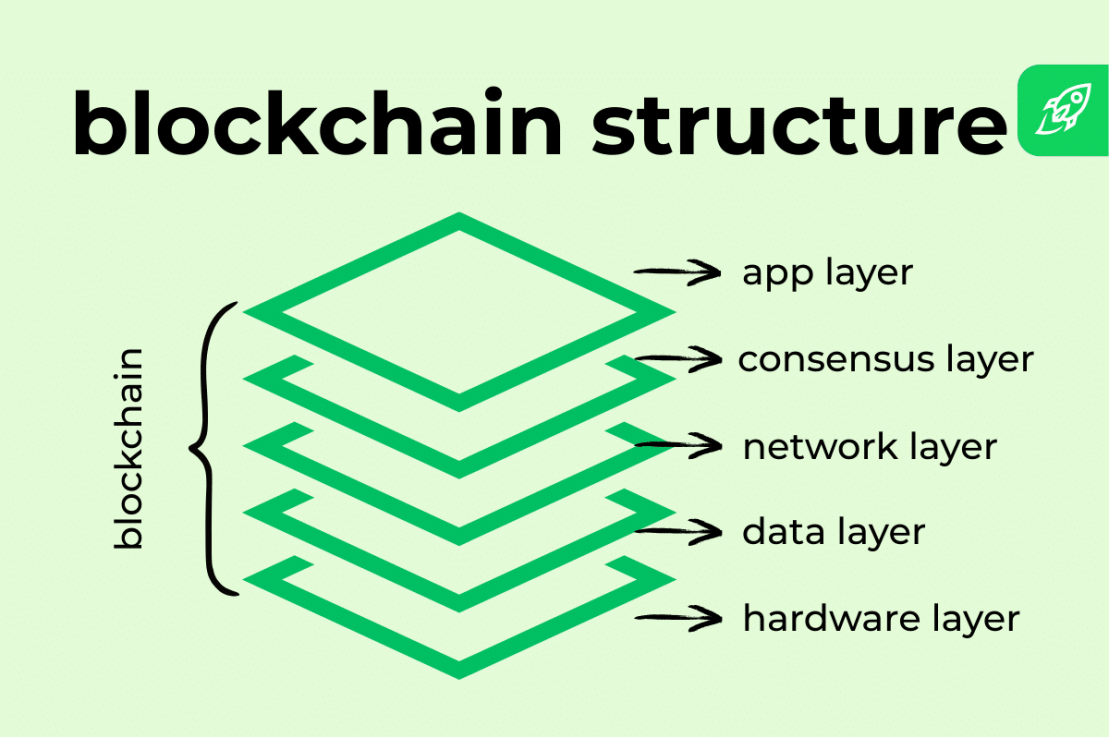
3.1.1 Το Θεώρημα CAP και η Εφαρμογή του στο Blockchain: Η αρχιτεκτονική του Blockchain διέπεται από το Θεώρημα CAP (Consistency, Availability, Partition Tolerance). Σε ένα κατανεμημένο σύστημα, είναι αδύνατο να επιτευχθούν ταυτόχρονα και οι τρεις ιδιότητες:

- Συνέπεια (Consistency): Όλοι οι κόμβοι βλέπουν τα ίδια δεδομένα την ίδια στιγμή.
- Διαθεσιμότητα (Availability): Το σύστημα ανταποκρίνεται πάντα στα αιτήματα.
- Ανοχή στον Διαχωρισμό (Partition Tolerance): Το σύστημα συνεχίζει να λειτουργεί ακόμα και αν κοπεί η επικοινωνία μεταξύ τμημάτων του δικτύου. Οι Zhou et al. (2021) αναλύουν ότι τα περισσότερα δημόσια Blockchains (όπως το Bitcoin) θυσιάζουν την άμεση *Συνέπεια* υπέρ της *Διαθεσιμότητας* και της *Ανοχής*, καταλήγοντας στο μοντέλο της "Τελικής Συνέπειας" (Eventual Consistency) [9].

3.2 Πολυεπίπεδη Αρχιτεκτονική (Layered Architecture)

Η σύγχρονη βιβλιογραφία (2021-2024) αποδομεί το Blockchain σε μια στοίβα τεσσάρων επιπέδων (Layers), αντί να το αντιμετωπίζει ως μονολιθικό σύστημα. Αυτή η προσέγγιση βοηθά στην κατανόηση των προβλημάτων επεκτασιμότητας.

- Layer 0 (Επίπεδο Υποδομής & Δικτύου): Περιλαμβάνει το φυσικό υλικό (servers, miners), το πρωτόκολλο διαδικτύου (TCP/IP) και το δίκτυο επικοινωνίας P2P. Εδώ ορίζεται πώς οι κόμβοι ανακαλύπτουν ο ένας τον άλλον και πώς μεταδίδονται τα πακέτα δεδομένων.
- Layer 1 (Επίπεδο Δεδομένων & Συναίνεσης): Είναι το "κυρίως" Blockchain (π.χ. Bitcoin, Ethereum Mainnet). Εδώ ορίζονται οι κανόνες του παιχνιδιού: η δομή των μπλοκ, η κρυπτογραφία και ο αλγόριθμος συναίνεσης (PoW, PoS). Σύμφωνα με τους Li et al. (2020), το Layer 1 είναι υπεύθυνο για την ασφάλεια και την αμετάβλητη καταγραφή [10].
- Layer 2 (Επίπεδο Επεκτασιμότητας): Περιλαμβάνει πρωτόκολλα που λειτουργούν "πάνω" από το Blockchain για να αυξήσουν την ταχύτητα (throughput). Παραδείγματα είναι το Lightning Network και τα Rollups (Optimistic & ZK-Rollups), τα οποία εκτελούν συναλλαγές εκτός αλυσίδας (off-chain) και δημοσιεύουν μόνο τα τελικά αποτελέσματα στο Layer 1.
- Layer 3 (Επίπεδο Εφαρμογής): Εδώ βρίσκονται οι Αποκεντρωμένες Εφαρμογές (DApps), τα ψηφιακά πορτοφόλια (Wallets) και οι διεπαφές χρήστη (UI) που επιτρέπουν την αλληλεπίδραση με τα έξυπνα συμβόλαια [11].



Εικόνα 3.1: Η λειτουργική αρχιτεκτονική στοίβα του Blockchain και τα βασικά της επίπεδα.

3.3 Δομή Δεδομένων: Το Μπλοκ και η Αλυσίδα

Το Blockchain πήρε το όνομά του από τη δομή του: μια γραμμική ακολουθία (αλυσίδα) από containers δεδομένων (μπλοκ). Κάθε μπλοκ συνδέεται κρυπτογραφικά με το προηγούμενο, δημιουργώντας μια αδιάσπαστη ιστορική συνέχεια.

3.3.1 Η Κεφαλίδα του Μπλοκ (Block Header): Η κεφαλίδα είναι το πιο κρίσιμο τμήμα, καθώς περιέχει τα μετα-δεδομένα. Σύμφωνα με την τεχνική ανάλυση των Casino et al. (2020), τα βασικά πεδία είναι:

1. Version: Έκδοση λογισμικού (για παρακολούθηση αναβαθμίσεων/forks).
2. Previous Block Hash: Η ψηφιακή υπογραφή του γονικού μπλοκ. Αυτό είναι το πεδίο που εξασφαλίζει το Immutability (Αμετάβλητο): αν κάποιος προσπαθήσει να αλλάξει μια συναλλαγή σε ένα παλιό μπλοκ, θα αλλάξει το hash του, ακυρώνοντας όλα τα επόμενα μπλοκ [12].
3. Merkle Root: Η ρίζα του δέντρου Merkle (βλ. παρακάτω).
4. Timestamp: Χρονική σήμανση (σε Unix time).
5. Difficulty Target (Bits): Ο στόχος δυσκολίας για την εξόρυξη.
6. Nonce: Ο τυχαίος αριθμός που χρησιμοποιείται στο Proof of Work.

3.3.2 Δέντρα Merkle (Merkle Trees) και SPV: Τα δέντρα Merkle αποτελούν τη θεμελιώδη δομή για την αποδοτική επαλήθευση δεδομένων. Κάθε συναλλαγή κατακερματίζεται (hashed) και συνδυάζεται με άλλες ανά ζεύγη, μέχρι να προκύψει ένα τελικό hash (Root). Η σημασία τους, όπως τονίζεται από τους Gai et al. (2020), είναι διττή:

- Ακεραιότητα: Κάθε αλλαγή σε συναλλαγή αλλάζει τη Ρίζα.
- Ελαφρύς Έλεγχος (SPV - Simplified Payment Verification): Επιτρέπει σε κινητά τηλέφωνα (Light Nodes) να επιβεβαιώσουν μια πληρωμή κατεβάζοντας μόνο την κεφαλίδα (80 bytes) και όχι τα GB όλης της αλυσίδας [13].

3.4 Μοντέλα Διαχείρισης Κατάστασης (State Models)

Η αρχιτεκτονική ενός Blockchain καθορίζεται θεμελιωδώς από τον τρόπο με τον οποίο το δίκτυο καταγράφει, αποθηκεύει και ενημερώνει την κατάσταση (state) των περιουσιακών στοιχείων των χρηστών. Στη σύγχρονη βιβλιογραφία, διακρίνονται δύο κυρίαρχα παραδείγματα (paradigms): το μοντέλο Μη Δαπανημένων Εξόδων Συναλλαγών (UTXO) και το Μοντέλο Βάσει Λογαριασμού (Account-Based).

3.4.1 Το Μοντέλο UTXO (Unspent Transaction Output): Το μοντέλο UTXO, το οποίο υιοθετήθηκε αρχικά από το Bitcoin και αργότερα από δίκτυα όπως το Litecoin και το Cardano (στο μοντέλο EUTXO), προσομοιάζει τη λειτουργία των μετρητών στον φυσικό κόσμο. Σε αυτό το σύστημα, δεν υπάρχουν "λογαριασμοί" με τρέχοντα υπόλοιπα σε επίπεδο πρωτοκόλλου. Αντ' αυτού, το καθολικό αποτελείται από ένα σύνολο διάσπαρτων "κερμάτων" (outputs) που ανήκουν σε συγκεκριμένες διευθύνσεις. Κάθε συναλλαγή καταναλώνει ένα ή περισσότερα προηγούμενα outputs (inputs) και δημιουργεί νέα (outputs). Για παράδειγμα, αν ένας χρήστης κατέχει ένα output αξίας 10 BTC και επιθυμεί να στείλει 2 BTC, πρέπει να "δαπανήσει" ολόκληρο το ποσό των 10 BTC ως είσοδο και να δημιουργήσει δύο νέες εξόδους: μία αξίας 2 BTC για τον παραλήπτη και μία αξίας 8 BTC ως "ρέστα" (change) που επιστρέφουν στον ίδιο.

Σύμφωνα με τους Chung et al. (2021), το κύριο πλεονέκτημα αυτής της προσέγγισης είναι η δυνατότητα παράλληλης επεξεργασίας συναλλαγών (parallelism), καθώς οι συναλλαγές που αφορούν διαφορετικά UTXOs είναι ανεξάρτητες μεταξύ τους, αυξάνοντας έτσι την επεκτασιμότητα του δικτύου. Επιπλέον, προσφέρει αυξημένη ιδιωτικότητα, καθώς ενθαρρύνει τη χρήση νέων διευθύνσεων για κάθε συναλλαγή (change addresses) [14].

3.4.2 Το Μοντέλο Λογαριασμού (Account-Based Model): Στον αντίποδα, το Μοντέλο Λογαριασμού, που χρησιμοποιείται από το Ethereum, το Solana και το Polkadot, λειτουργεί με τρόπο παρόμοιο με τις παραδοσιακές τραπεζικές βάσεις δεδομένων. Το δίκτυο διατηρεί μια παγκόσμια κατάσταση (Global State) που περιλαμβάνει μια αντιστοίχιση διευθύνσεων προς τα τρέχοντα υπόλοιπά τους. Σε αυτό το πλαίσιο, μια συναλλαγή δεν καταστρέφει προηγούμενα outputs, αλλά αποτελεί μια εντολή μετάβασης κατάστασης (state transition) που χρεώνει τον λογαριασμό του αποστολέα και πιστώνει τον λογαριασμό του παραλήπτη. Για την αποφυγή επιθέσεων επανάληψης (replay attacks), κάθε λογαριασμός διατηρεί έναν αυξανόμενο αριθμό σειράς (nonce).

Όπως επισημαίνουν οι Wang et al. (2021), το βασικό πλεονέκτημα αυτού του μοντέλου είναι η απλότητα στην ανάπτυξη πολύπλοκων Έξυπνων Συμβολαίων (Smart Contracts). Δεδομένου ότι τα DApps απαιτούν συχνά την παρακολούθηση της κατάστασης ενός χρήστη σε βάθος χρόνου (π.χ. σε πρωτόκολλα δανεισμού DeFi), το μοντέλο λογαριασμού είναι πιο αποδοτικό στη διαχείριση μνήμης, καθώς απαιτεί λιγότερο αποθηκευτικό χώρο σε σύγκριση με το UTXO [11].

3.4.3 Συγκριτική Ανάλυση των Μοντέλων UTXO και Λογαριασμού: Η επιλογή μεταξύ του μοντέλου UTXO και του μοντέλου Λογαριασμού (Account-Based) δεν αποτελεί απλώς μια σχεδιαστική λεπτομέρεια, αλλά μια θεμελιώδη αρχιτεκτονική απόφαση που καθορίζει τις δυνατότητες, την ασφάλεια και την απόδοση του εκάστοτε Blockchain. Η βιβλιογραφία εντοπίζει πέντε κρίσιμους τομείς διαφοροποίησης: τη θεμελιώδη μονάδα δεδομένων, την επεκτασιμότητα, την ιδιωτικότητα, την προγραμματισιμότητα και την ασφάλεια έναντι της διπλής δαπάνης.

Α. Θεμελιώδης Μονάδα Δεδομένων (Basic Unit) Στο μοντέλο UTXO (Bitcoin, Cardano), η βασική μονάδα είναι το ίδιο το "κέρμα" ή πιο σωστά, η Μη Δαπανημένη Έξοδος. Το σύστημα δεν αντιλαμβάνεται την έννοια του συνολικού "υπολοίπου" ενός χρήστη. Αντίθετα, αντιλαμβάνεται ένα σύνολο διάσπαρτων κερμάτων που ανήκουν σε ένα κλειδί. Για να πραγματοποιηθεί μια συναλλαγή, ο χρήστης πρέπει να συλλέξει αυτά τα κέρματα και να τα δαπανήσει αθροιστικά.

Αντίθετα, στο Μοντέλο Λογαριασμού (Ethereum, Solana), η βασική μονάδα είναι η ολότητα του Λογαριασμού. Το σύστημα λειτουργεί ως μια παγκόσμια βάση δεδομένων ζευγών "Κλειδί-Τιμή" (Key-Value store), όπου κάθε διεύθυνση συνδέεται άμεσα με μια αριθμητική τιμή που αντιπροσωπεύει το υπόλοιπο. Η συναλλαγή εδώ δεν είναι μεταφορά φυσικών αντικειμένων (όπως στο UTXO), αλλά μια εντολή ενημέρωσης λογιστικής εγγραφής [14].

Β. Επεκτασιμότητα και Παράλληλη Επεξεργασία (Scalability) Ίσως η πιο σημαντική τεχνική διαφορά αφορά τη δυνατότητα παράλληλης επεξεργασίας.

- Στο μοντέλο UTXO, οι συναλλαγές είναι εκ φύσεως ανεξάρτητες μεταξύ τους, εφόσον καταναλώνουν διαφορετικές εξόδους. Αυτό επιτρέπει στους κόμβους να επαληθεύουν πολλαπλές συναλλαγές ταυτόχρονα (parallel verification), εκμεταλλευόμενοι τους πολυπύρηνους επεξεργαστές. Αυτό καθιστά το μοντέλο UTXO εξαιρετικά επεκτάσιμο για απλές πληρωμές.
- Στο μοντέλο Λογαριασμού, κάθε συναλλαγή που αφορά έναν συγκεκριμένο λογαριασμό εξαρτάται από την προηγούμενη κατάστασή του (π.χ. το υπόλοιπο πρέπει να είναι επαρκές *μετά* την προηγούμενη χρέωση). Αυτό δημιουργεί μια εξάρτηση που επιβάλλει τη σειριακή εκτέλεση των συναλλαγών (sequential processing), δημιουργώντας συχνά φαινόμενα συμφόρησης (bottlenecks) στο δίκτυο [9].

Γ. Ιδιωτικότητα και Ανωνυμία (Privacy) Το μοντέλο UTXO προσφέρει εγγενώς υψηλότερο επίπεδο ιδιωτικότητας. Καθώς κάθε συναλλαγή δημιουργεί νέα outputs, τα πορτοφόλια ενθαρρύνουν τη χρήση νέων διευθύνσεων για τα "ρέστα" (change addresses). Έτσι, ένας χρήστης μπορεί να έχει τα κεφάλαιά του μοιρασμένα σε δεκάδες διαφορετικές διευθύνσεις, καθιστώντας δύσκολη τη συσχέτισή τους από τρίτους παρατηρητές (chain analysis). Στο Μοντέλο Λογαριασμού, η πρακτική αυτή είναι δυσκολότερη και κοστοβόρα. Οι χρήστες τείνουν να χρησιμοποιούν μία σταθερή διεύθυνση για όλες τις συναλλαγές τους, λειτουργώντας ως "τραπεζικός λογαριασμός". Αυτό έχει ως αποτέλεσμα όλη η οικονομική ιστορία του χρήστη να είναι διαφανής και εύκολα ιχνηλασιμη στο Blockchain explorer.

Δ. Προγραμματισιμότητα και Έξυπνα Συμβόλαια (Programmability) Εδώ έγκειται το μεγάλο πλεονέκτημα του Μοντέλου Λογαριασμού. Επειδή διατηρεί μια παγκόσμια κατάσταση, είναι πολύ εύκολο για έναν προγραμματιστή να γράψει κώδικα (Smart Contract) που ελέγχει συνθήκες όπως *"Αν το υπόλοιπο του Χ > 100, τότε κάνε Υ"*. Είναι Turing-complete και φιλικό προς την ανάπτυξη πολύπλοκων εφαρμογών (DApps). Αντίθετα, το μοντέλο UTXO είναι "stateless" (χωρίς μνήμη κατάστασης). Κάθε συναλλαγή βλέπει μόνο τις εισόδους της και τίποτα άλλο. Αυτό καθιστά εξαιρετικά δύσκολη την ανάπτυξη εφαρμογών που απαιτούν αλληλεπίδραση πολλών χρηστών (π.χ. ένα αποκεντρωμένο ανταλλακτήριο - DEX), αν και νεότερες υλοποιήσεις (όπως το eUTXO του Cardano) προσπαθούν να γεφυρώσουν αυτό το χάσμα [11].

Ε. Ασφάλεια Έναντι Διπλής Δαπάνης (Double Spending) Και τα δύο μοντέλα λύνουν το πρόβλημα της διπλής δαπάνης, αλλά με διαφορετικούς μηχανισμούς:

- Το UTXO χρησιμοποιεί έναν απλό έλεγχο ύπαρξης: *"Υπάρχει αυτό το output στα αδιάθετα; Αν ναι, ξόδεψέ το και διάγραψέ το. Αν όχι, η συναλλαγή είναι άκυρη"*.
- Το Account Model χρησιμοποιεί έναν μετρητή σειράς που ονομάζεται Nonce. Κάθε συναλλαγή πρέπει να έχει έναν μοναδικό αριθμό nonce (π.χ. 1, 2, 3...). Αν το δίκτυο λάβει δύο συναλλαγές με το ίδιο nonce, αποδέχεται μόνο την πρώτη και απορρίπτει τη δεύτερη, αποτρέποντας έτσι την επανάληψη συναλλαγών (replay attacks) και τη διπλή δαπάνη.

ΠΙΝΑΚΑΣ 1: Μοντέλο UTXO έναντι Μοντέλου Λογαριασμού

Χαρακτηριστικό	Μοντέλο UTXO (π.χ. Bitcoin)	Μοντέλο Λογαριασμού (π.χ. Ethereum)
Βασική Μονάδα	Μη-Δαπανημένη Έξοδος (Κέρμα)	Λογαριασμός / Υπόλοιπο (Balance)
Παράλληλη Επεξεργασία	Εύκολη (ανεξάρτητα UTXOs)	Δύσκολη (απαιτείται σειριακή εκτέλεση)
Ιδιωτικότητα	Υψηλότερη (χρήση change addresses)	Χαμηλότερη (σταθερή διεύθυνση)
Έξυπνα Συμβόλαια	Δύσκολη υλοποίηση (Stateless)	Φιλικό (Turing-complete, Stateful)
Αποτροπή Διπλής Δαπάνης	Έλεγχος διαθεσιμότητας εξόδου	Έλεγχος αύξοντος αριθμού (Nonce)

3.5 Δίκτυα Peer-to-Peer και Πρωτόκολλα Διάδοσης

Το δίκτυο Blockchain είναι ένα "mesh" δίκτυο χωρίς κεντρικούς διακομιστές.

3.5.1 Τυπολογία Κόμβων (Node Taxonomy): Σύμφωνα με τους Xiao et al. (2020), οι ρόλοι στο δίκτυο διακρίνονται ως εξής:

- Full Nodes (Πλήρεις Κόμβοι): Κατέχουν όλο το ιστορικό και επαληθεύουν κάθε κανόνα. Είναι οι θεματοφύλακες του δικτύου.
- Pruned Nodes: Πλήρεις κόμβοι που διαγράφουν τα πολύ παλιά δεδομένα για να εξοικονομήσουν χώρο στον δίσκο, κρατώντας μόνο τα τελευταία GB.
- Archival Nodes: Κρατούν τα πάντα, ακόμα και δεδομένα που δεν είναι πλέον απαραίτητα για την τρέχουσα λειτουργία (χρήσιμοι για explorers και αναλυτές).
- Miners/Validators: Κόμβοι που παράγουν νέα μπλοκ.

3.5.2 Gossip Protocols: Η πληροφορία διαδίδεται μέσω πρωτοκόλλων "κουτσομπολιού". Όταν ένας κόμβος μαθαίνει για μια νέα συναλλαγή, την ελέγχει και την στέλνει στους 8-10 γείτονές του. Η διαδικασία επαναλαμβάνεται εκθετικά. Πρόσφατες έρευνες εστιάζουν στη βελτιστοποίηση αυτών των πρωτοκόλλων (π.χ. Erlay protocol στο Bitcoin) για τη μείωση του bandwidth [15].

3.6 Τυπολογία και Ταξινόμηση Δικτύων Blockchain

Η βιβλιογραφία ταξινομεί τα δίκτυα Blockchain με βάση δύο κύριους άξονες: το δικαίωμα ανάγνωσης (ποιος βλέπει τις συναλλαγές) και το δικαίωμα εγγραφής/επικύρωσης (ποιος παράγει

τα μπλοκ). Σύμφωνα με τους Wegrzyn & Wang (2021), η διάκριση αυτή καθορίζει την αρχιτεκτονική ασφαλείας και το πεδίο εφαρμογής του κάθε συστήματος [16].

3.6.1 Δημόσια Δίκτυα (Public / Permissionless Blockchains): Στα δημόσια δίκτυα, η συμμετοχή είναι ελεύθερη και ανώνυμη (ή ψευδώνυμη). Δεν υπάρχει κεντρική αρχή που να εγκρίνει την είσοδο νέων κόμβων. Οποιοσδήποτε χρήστης μπορεί να κατεβάσει το λογισμικό, να διαβάσει το καθολικό και να συμμετάσχει στη διαδικασία συναίνεσης.

- Χαρακτηριστικά: Η ασφάλεια βασίζεται σε μηχανισμούς κρυπτοοικονομικών κινήτρων (Game Theory) και μαθηματικής πολυπλοκότητας (π.χ. Proof of Work), καθώς δεν υπάρχει εμπιστοσύνη μεταξύ των κόμβων. Αυτό οδηγεί σε υψηλή αποκέντρωση και αντίσταση στη λογοκρισία, αλλά μειώνει δραματικά την ταχύτητα επεξεργασίας.
- Παράδειγμα 1 - Bitcoin (BTC): Αποτελεί το αρχέτυπο του δημόσιου Blockchain. Η ασφάλειά του εξασφαλίζεται από την τεράστια δεξαμενή υπολογιστικής ισχύος (hashrate) που καθιστά οικονομικά ασύμφορη οποιαδήποτε επίθεση. Είναι βελτιστοποιημένο για ασφάλεια και όχι για ταχύτητα (μόλις 7 συναλλαγές/δευτερόλεπτο).
- Παράδειγμα 2 - Ethereum (ETH): Λειτουργεί ως δημόσια υποδομή για την εκτέλεση Έξυπνων Συμβολαίων. Επιτρέπει σε προγραμματιστές να χτίσουν εφαρμογές (DApps) χωρίς να ζητήσουν άδεια από κανέναν ("permissionless innovation").

3.6.2 Ιδιωτικά Δίκτυα (Private / Permissioned Blockchains): Τα ιδιωτικά δίκτυα λειτουργούν σε κλειστά περιβάλλοντα, συνήθως εντός ενός οργανισμού. Η πρόσβαση ελέγχεται αυστηρά από μια κεντρική αρχή διαχείρισης (Network Administrator) μέσω Λιστών Ελέγχου Πρόσβασης (Access Control Lists - ACLs). Οι συμμετέχοντες είναι γνωστές και ταυτοποιημένες οντότητες.

- Χαρακτηριστικά: Επειδή υπάρχει εμπιστοσύνη (ή νομική σύμβαση) μεταξύ των κόμβων, δεν απαιτούνται βαριοί αλγόριθμοι όπως το Proof of Work. Χρησιμοποιούνται ελαφρύτεροι μηχανισμοί (π.χ. Raft, Paxos), επιτυγχάνοντας χιλιάδες συναλλαγές ανά δευτερόλεπτο με αμελητέο κόστος.
- Παράδειγμα - Hyperledger Fabric: Ένα έργο του Linux Foundation που χρησιμοποιείται ευρέως στην εφοδιαστική αλυσίδα (Supply Chain). Επιτρέπει τη δημιουργία "καναλιών" (channels) όπου τα δεδομένα είναι ορατά μόνο σε συγκεκριμένους συμμετέχοντες, διασφαλίζοντας το επιχειρηματικό απόρρητο.
- Παράδειγμα - Quorum: Αναπτύχθηκε από την JP Morgan (βασισμένο στο Ethereum) για διατραπεζικές συναλλαγές, προσφέροντας ιδιωτικότητα σε επίπεδο συναλλαγής.

3.6.3 Κοινοπρακτικά Δίκτυα (Consortium / Federated Blockchains): Τα κοινοπρακτικά δίκτυα αποτελούν μια υβριδική λύση που γεφυρώνει το χάσμα μεταξύ των δύο προηγούμενων κατηγοριών. Εδώ, ο έλεγχος δεν ανήκει σε μία μόνο οντότητα, αλλά σε μια προεπιλεγμένη ομάδα οργανισμών (π.χ. μια ένωση 15 τραπεζών).

- Χαρακτηριστικά: Η διαδικασία συναίνεσης ελέγχεται από ένα σύνολο "κόμβων επικύρωσης" (validator nodes). Για να εγκριθεί ένα μπλοκ, απαιτείται η ψηφιακή υπογραφή της πλειοψηφίας των μελών (π.χ. 10 από τους 15). Αυτό το μοντέλο μειώνει τον κίνδυνο μονοπωλίου (που υπάρχει στα ιδιωτικά δίκτυα) ενώ διατηρεί υψηλή ταχύτητα.

- Παράδειγμα - R3 Corda: Μια πλατφόρμα DLT σχεδιασμένη αποκλειστικά για τον χρηματοπιστωτικό τομέα. Σε αντίθεση με τα παραδοσιακά Blockchains, στο Corda τα δεδομένα δεν κοινοποιούνται σε όλους τους κόμβους, αλλά μόνο στα μέρη που εμπλέκονται στη συναλλαγή, προσφέροντας νομική συμμόρφωση και ιδιωτικότητα.
- Παράδειγμα - Energy Web Chain: Μια κοινοπραξία ενεργειακών εταιρειών (Shell, Siemens, κ.ά.) που χρησιμοποιεί Blockchain για την αποκεντρωμένη διαχείριση του ηλεκτρικού δικτύου.

3.6.4 Συγκριτική Αξιολόγηση Επιδόσεων και Χαρακτηριστικών: Η επιλογή της κατάλληλης αρχιτεκτονικής Blockchain δεν είναι μονοσήμαντη, αλλά εξαρτάται από τις ειδικές απαιτήσεις της εκάστοτε εφαρμογής. Σύμφωνα με τη συγκριτική ανάλυση των Casino et al. (2020) και Wegrzyn & Wang (2021), παρατηρείται μια σαφής σχέση αντιστροφής (trade-off) μεταξύ της αποκέντρωσης και της απόδοσης του συστήματος. Η βιβλιογραφία διακρίνει τις διαφορές στους εξής πέντε βασικούς άξονες:

Α. Πρόσβαση και Συμμετοχή Στα Δημόσια Δίκτυα (Public), η πρόσβαση είναι καθολική και χωρίς περιορισμούς (permissionless). Οποιοσδήποτε χρήστης με σύνδεση στο διαδίκτυο μπορεί να εγγράψει δεδομένα στο καθολικό και να συμμετάσχει στη διαδικασία επικύρωσης. Αντιθέτως, στα Ιδιωτικά (Private) και Κοινοπρακτικά (Consortium) δίκτυα, η συμμετοχή είναι ελεγχόμενη (permissioned). Απαιτείται ρητή εξουσιοδότηση από τον διαχειριστή του δικτύου ή την κοινοπραξία, γεγονός που τα καθιστά κατάλληλα για εταιρικά περιβάλλοντα όπου η ταυτοποίηση των χρηστών (Know Your Customer - KYC) είναι υποχρεωτική [12].

Β. Ταχύτητα και Διεκπεραίωση Συναλλαγών (Throughput) Υπάρχει χαώδης διαφορά στην ταχύτητα επεξεργασίας.

- Τα Δημόσια Δίκτυα (όπως το Bitcoin και το Ethereum Layer 1) χαρακτηρίζονται από χαμηλή απόδοση (περίπου 7 έως 15 συναλλαγές ανά δευτερόλεπτο). Αυτό οφείλεται στην ανάγκη επίτευξης συναίνεσης μεταξύ χιλιάδων άγνωστων κόμβων παγκοσμίως, καθώς και στους μηχανισμούς ασφαλείας που επιβάλλουν τεχνητές καθυστερήσεις (block time).
- Στον αντίποδα, τα Ιδιωτικά και Κοινοπρακτικά Δίκτυα επιτυγχάνουν εξαιρετικά υψηλές ταχύτητες, που συχνά υπερβαίνουν τις 10.000 συναλλαγές ανά δευτερόλεπτο (TPS). Αυτό συμβαίνει διότι οι κόμβοι είναι λίγοι, γνωστοί και εμπίστοι, επιτρέποντας τη χρήση ταχύτερων αλγορίθμων συναίνεσης (όπως οι Paxos, Raft ή PBFT) που δεν απαιτούν πολύπλοκους υπολογισμούς [16].

Γ. Βαθμός Αποκέντρωσης και Διακυβέρνηση Η αποκέντρωση είναι το κύριο πλεονέκτημα των δημόσιων δικτύων. Δεν υπάρχει "ιδιοκτήτης" ή κεντρικό σημείο αποτυχίας, καθιστώντας το δίκτυο ανθεκτικό στη λογοκρισία και τις επιθέσεις. Στα Κοινοπρακτικά δίκτυα, η διακυβέρνηση είναι "πολυκεντρική" (polycentric), καθώς οι αποφάσεις λαμβάνονται από μια ομάδα οργανισμών, μειώνοντας τον κίνδυνο μονοπωλίου αλλά χωρίς να τον εξαλείφουν πλήρως. Τέλος, τα Ιδιωτικά δίκτυα είναι πλήρως κεντρικοποιημένα, καθώς ένας μοναδικός οργανισμός έχει τον πλήρη έλεγχο, προσομοιάζοντας ουσιαστικά μια παραδοσιακή βάση δεδομένων με κρυπτογραφικές υπογραφές.

Δ. Αμετάβλητο των Δεδομένων (Immutability) Στα δημόσια Blockchain, η τροποποίηση του ιστορικού συναλλαγών είναι πρακτικά αδύνατη, καθώς θα απαιτούσε τεράστια υπολογιστική ισχύ (επίθεση 51%). Αυτό προσφέρει την υψηλότερη δυνατή ασφάλεια. Αντίθετα, στα ιδιωτικά και κοινοπρακτικά δίκτυα, το "αμετάβλητο" είναι σχετικό. Εάν η πλειοψηφία των συμμετεχόντων οργανισμών συμφωνήσει (π.χ. λόγω ενός νομικού σφάλματος), μπορούν να αποφασίσουν συντονισμένα την αναστροφή συναλλαγών ή την τροποποίηση του καθολικού.

Ε. Ενεργειακή Κατανάλωση Τα δημόσια δίκτυα που βασίζονται στο Proof of Work (όπως το Bitcoin) έχουν δεχθεί έντονη κριτική για την τεράστια κατανάλωση ενέργειας. Αντιθέτως, τα ιδιωτικά και κοινοπρακτικά δίκτυα είναι φιλικά προς το περιβάλλον ("Green Blockchains"), καθώς

οι αλγόριθμοι συναίνεσης που χρησιμοποιούν απαιτούν αμελητέα επεξεργαστική ισχύ, παρόμοια με αυτήν ενός απλού διακομιστή web.

ΚΕΦΑΛΑΙΟ 4: ΚΡΥΠΤΟΓΡΑΦΙΚΕΣ ΥΠΟΔΟΜΕΣ ΚΑΙ ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ

4.1 Ο Ρόλος της Κρυπτογραφίας σε Περιβάλλοντα Μηδενικής Εμπιστοσύνης

Στα συμβατικά πληροφοριακά συστήματα, η ασφάλεια βασίζεται στο μοντέλο της "περιμετρικής άμυνας" (firewalls, IDS) και της κεντρικής διαχείρισης ταυτοτήτων (IAM). Ωστόσο, στα αποκεντρωμένα δίκτυα Blockchain, όπου το περιβάλλον είναι εξ ορισμού "εχθρικό" (adversarial) και οι κόμβοι ανώνυμοι, το μοντέλο αυτό καταρρέει. Σύμφωνα με τους Gai et al. (2020) και Li et al. (2020), η κρυπτογραφία αναλαμβάνει να υποκαταστήσει την ανάγκη για ανθρώπινη εμπιστοσύνη, εξυπηρετώντας τρεις θεμελιώδεις στόχους, οι οποίοι επαναπροσδιορίζονται ως εξής [10, 17]:

4.1.1 Ακεραιότητα Δεδομένων (Data Integrity): Σε μια κεντρική βάση δεδομένων, η ακεραιότητα εξαρτάται από τον διαχειριστή. Στο Blockchain, η ακεραιότητα είναι μαθηματικά εγγυημένη και αφορά την εξασφάλιση ότι τα δεδομένα των συναλλαγών δεν έχουν παραποιηθεί από τη στιγμή της δημιουργίας τους. Αυτό επιτυγχάνεται μέσω δύο μηχανισμών:

- Αμετάβλητο Ιστορικό: Κάθε μπλοκ περιέχει το κρυπτογραφικό αποτύπωμα (hash) του προηγούμενου. Οποιαδήποτε απόπειρα τροποποίησης μιας συναλλαγής του παρελθόντος (π.χ. αλλαγή ποσού) θα άλλαζε το hash του μπλοκ, σπάζοντας την αλυσίδα των δεικτών και καθιστώντας την απάτη άμεσα ανιχνεύσιμη από όλο το δίκτυο.
- Ατομική Ακεραιότητα: Κάθε συναλλαγή προστατεύεται ξεχωριστά. Το hash της συναλλαγής λειτουργεί ως ένα μοναδικό αναγνωριστικό (TXID). Εάν αλλάξει έστω και ένα bit στα δεδομένα της συναλλαγής, το TXID αλλάζει δραματικά (φαινόμενο χιονοστιβάδας), ακυρώνοντας τη συναλλαγή.

4.1.2 Μη-Αρνησιμότητα (Non-Repudiation): Η μη-αρνησιμότητα είναι η ιδιότητα που εμποδίζει έναν χρήστη να αρνηθεί εκ των υστέρων ότι πραγματοποίησε μια ενέργεια. Στα παραδοσιακά συστήματα, αυτό επιτυγχάνεται μέσω καταγραφής logs (audit trails). Στα κρυπτονομίσματα, επιτυγχάνεται μέσω των Ψηφιακών Υπογραφών (Digital Signatures). Όταν ένας χρήστης στέλνει κρυπτονομίσματα, υπογράφει τη συναλλαγή με το Ιδιωτικό του Κλειδί (Private Key). Επειδή το κλειδί αυτό είναι μαθηματικά μοναδικό και βρίσκεται αποκλειστικά στην κατοχή του χρήστη, η ύπαρξη μιας έγκυρης υπογραφής στο δίκτυο αποτελεί αδιάσειστη απόδειξη ότι η εντολή προήλθε από τον συγκεκριμένο χρήστη. Κανείς δεν μπορεί να πλαστογραφήσει την υπογραφή χωρίς το ιδιωτικό κλειδί και ο χρήστης δεν μπορεί να ισχυριστεί ότι "δεν το έκανε αυτός".

4.1.3 Αυθεντικοποίηση Χωρίς Ταυτότητα (Authentication without Identity): Η πιο ριζοσπαστική διαφορά του Blockchain είναι ο διαχωρισμός της "ταυτότητας" από την "ιδιοκτησία". Στον φυσικό κόσμο, η αυθεντικοποίηση απαιτεί την αποκάλυψη του "ποιος είσαι" (π.χ. επίδειξη ταυτότητας). Στο Blockchain, η αυθεντικοποίηση αφορά το "τι ξέρεις".

- Απόδειξη Ιδιοκτησίας: Το δίκτυο δεν ενδιαφέρεται για το όνομα του χρήστη, αλλά μόνο για το αν κατέχει το κλειδί που ξεκλειδώνει τα κεφάλαια (Unspent Outputs). Η κατοχή του Ιδιωτικού Κλειδιού είναι η μόνη μορφή αυθεντικοποίησης.
- Ψευδωνυμία: Αυτός ο μηχανισμός επιτρέπει στους χρήστες να αλληλεπιδρούν με ασφάλεια χωρίς να γνωρίζονται μεταξύ τους. Η εμπιστοσύνη μεταφέρεται από το πρόσωπο στα μαθηματικά της κρυπτογραφίας ("In Cryptography We Trust").

4.2 Κρυπτογραφικές Συναρτήσεις Κατακερματισμού (Hash Functions)

Οι συναρτήσεις κατακερματισμού αποτελούν τον ακρογωνιαίο λίθο της δομής του Blockchain. Πρόκειται για μονόδρομες συναρτήσεις (one-way functions) που μετατρέπου δεδομένα οποιουδήποτε μεγέθους σε μια συμβολοσειρά σταθερού μήκους (digest).

4.2.1 Ιδιότητες Ασφαλείας και Φαινόμενο Χιονοστιβάδας: Για να θεωρηθεί ένας αλγόριθμος ασφαλής για χρήση σε κρυπτονομίσματα, η σύγχρονη βιβλιογραφία απαιτεί την αυστηρή τήρηση τριών ιδιοτήτων:

- Αντίσταση στην Προ-εικόνα (Pre-image Resistance): Δεδομένου του hash h, είναι υπολογιστικά αδύνατο να βρεθεί το μήνυμα m.
- Αντίσταση στη Σύγκρουση (Collision Resistance): Είναι αδύνατο να βρεθούν δύο διαφορετικά μηνύματα m1 ≠ m2 που να παράγουν το ίδιο hash.
- Φαινόμενο της Χιονοστιβάδας (Avalanche Effect): Μια αλλαγή σε ένα μόνο bit της εισόδου πρέπει να αλλάζει κατά μέσο όρο το 50% των bits της εξόδου. Αυτή η ιδιότητα εμποδίζει τους επιτιθέμενους να προβλέψουν το hash ή να βρουν μοτίβα [18].

4.2.2 Συγκριτική Ανάλυση: SHA-256 vs SHA-3 (Keccak): Τα δύο κυρίαρχα πρότυπα στον χώρο είναι το SHA-256 (Bitcoin family) και το Keccak-256 (Ethereum family).

- SHA-256: Ανήκει στην οικογένεια SHA-2 και χρησιμοποιεί τη δομή Merkle-Damgård. Παρά το γεγονός ότι είναι ασφαλές, είναι ευάλωτο σε επιθέσεις επέκτασης μήκους (length extension attacks), γι' αυτό και το Bitcoin εφαρμόζει διπλό hashing (SHA256(SHA256(x))).
- SHA-3 (Keccak): Χρησιμοποιεί τη δομή "Sponge" (σφουγγάρι). Σύμφωνα με τους Liu et al. (2021), το SHA-3 προσφέρει υψηλότερη ασφάλεια και ταχύτητα σε υλοποιήσεις hardware (ASICs), ενώ είναι εγγενώς ανθεκτικό σε επιθέσεις επέκτασης μήκους χωρίς την ανάγκη διπλής εφαρμογής [19].

4.3 Ασύμμετρη Κρυπτογραφία και Ελλειπτικές Καμπύλες (ECC)

Ενώ το διαδίκτυο βασίστηκε για δεκαετίες στον αλγόριθμο RSA, τα κρυπτονομίσματα υιοθέτησαν σχεδόν καθολικά την Κρυπτογραφία Ελλειπτικών Καμπυλών (ECC).

4.3.1 Το Πρόβλημα του Διακριτού Λογαρίθμου (ECDLP): Η ασφάλεια της ECC βασίζεται στη δυσκολία επίλυσης του προβλήματος του διακριτού λογαρίθμου σε ομάδα σημείων μιας ελλειπτικής καμπύλης.

Η εξίσωση ορίζεται ως $Q = k \times G$, όπου:

- k: Το Ιδιωτικό Κλειδί (ένας τυχαίος ακέραιος).
- G: Το Σημείο Γεννήτορας (γνωστό σε όλους).
- Q: Το Δημόσιο Κλειδί.

Ενώ ο πολλαπλασιασμός (παραγωγή του Q από το k) είναι εύκολος, η αντίστροφη πράξη (εύρεση του k από το Q) είναι υπολογιστικά ανέφικτη με τα σημερινά μέσα.

4.3.2 Συγκριτική Ανάλυση Αποδοτικότητας: RSA έναντι ECC: Η επικράτηση της Κρυπτογραφίας Ελλειπτικών Καμπυλών (ECC) έναντι του παραδοσιακού αλγορίθμου RSA στα κρυπτονομίσματα δεν είναι τυχαία, αλλά αποτέλεσμα της ανάγκης για βελτιστοποίηση πόρων. Σύμφωνα με τους Zhang et al. (2021), η βασική διαφορά έγκειται στο μέγεθος του κλειδιού που απαιτείται για την επίτευξη ενός συγκεκριμένου επιπέδου ασφαλείας. Καθώς το πρόβλημα της παραγοντοποίησης (στο οποίο βασίζεται ο RSA) είναι υπολογιστικά ευκολότερο από το πρόβλημα του διακριτού λογαρίθμου σε ελλειπτικές καμπύλες (ECDLP), ο RSA απαιτεί εκθετικά μεγαλύτερα κλειδιά για να παραμείνει ασφαλής [20].

Αναλυτικότερα, για την παροχή ασφάλειας επιπέδου 80 bits, ο αλγόριθμος RSA απαιτεί κλειδί μεγέθους 1024 bits, ενώ η ECC επιτυγχάνει το ίδιο αποτέλεσμα με κλειδί μόλις 160 bits (λόγος 1:6). Καθώς οι απαιτήσεις ασφαλείας αυξάνονται, η ψαλίδα ανοίγει δραματικά. Για ασφάλεια επιπέδου 112 bits, ο RSA χρειάζεται 2048 bits, έναντι 224 bits της ECC.

Το πιο κρίσιμο σημείο σύγκρισης αφορά το επίπεδο ασφαλείας των 128 bits, το οποίο θεωρείται το ελάχιστο αποδεκτό πρότυπο για τα σύγχρονα κρυπτονομίσματα όπως το Bitcoin. Σε αυτό το επίπεδο, ο RSA απαιτεί ένα τεράστιο κλειδί 3072 bits, το οποίο είναι δυσκίνητο στην αποθήκευση και τη μετάδοση. Αντιθέτως, η ECC προσφέρει την ίδια αδιαπέραστη ασφάλεια με κλειδί μόλις 256 bits (λόγος 1:12). Αυτή η διαφορά μεγέθους είναι καθοριστική για την απόδοση του Blockchain, καθώς μικρότερα κλειδιά σημαίνουν μικρότερες συναλλαγές, λιγότερο απαιτούμενο χώρο στο καθολικό και ταχύτερη επαλήθευση από επεξεργαστές περιορισμένης ισχύος, όπως αυτοί των κινητών τηλεφώνων.

Τέλος, για στρατιωτικού επιπέδου ασφάλεια 256 bits, η υπεροχή της ECC γίνεται συντριπτική: απαιτεί κλειδί 512 bits, ενώ ο RSA θα χρειαζόταν το πρακτικά μη διαχειρίσιμο μέγεθος των 15.360 bits.

4.3.3 Η Καμπύλη secp256k1: Το Bitcoin χρησιμοποιεί την καμπύλη secp256k1 (Koblitz curve), η οποία ορίζεται από την εξίσωση:

$$y^2 = x^3 + 7 \ (mod\ p)$$

Η επιλογή αυτή, αντί της τυπικής secp256r1 του NIST, έγινε για να αποφευχθεί η πιθανότητα ύπαρξης κερκόπορτας (backdoor) από την NSA, καθώς οι παράμετροι της Koblitz curve είναι μαθηματικά προβλέψιμες και όχι τυχαίες [20].

4.4 Μηχανισμοί Ψηφιακών Υπογραφών (Digital Signature Schemes)

Η ψηφιακή υπογραφή αποτελεί το κρυπτογραφικό ισοδύναμο της χειρόγραφης υπογραφής, με τη θεμελιώδη διαφορά ότι είναι δυναμική: εξαρτάται τόσο από τον υπογράφοντα όσο και από το ίδιο το μήνυμα. Στο πλαίσιο των κρυπτονομισμάτων, η υπογραφή εξυπηρετεί δύο σκοπούς:

1. Απόδειξη Ιδιοκτησίας: Επιβεβαιώνει ότι ο εντολέας της συναλλαγής κατέχει το Ιδιωτικό Κλειδί που αντιστοιχεί στη διεύθυνση των κεφαλαίων.
2. Ακεραιότητα Μηνύματος: Εγγυάται ότι τα στοιχεία της συναλλαγής (ποσό, παραλήπτης) δεν τροποποιήθηκαν κατά τη μετάδοση.

Η βιβλιογραφία της τελευταίας πενταετίας εστιάζει στην εξέλιξη από τον παραδοσιακό αλγόριθμο ECDSA στον πιο σύγχρονο Schnorr, καθώς και στην υιοθέτηση του EdDSA σε blockchains νέας γενιάς.

4.4.1 Ο Αλγόριθμος ECDSA (Elliptic Curve Digital Signature Algorithm): Ο ECDSA αποτελεί το πρότυπο που υιοθετήθηκε αρχικά από το Bitcoin και το Ethereum. Η ασφάλειά του βασίζεται στο πρόβλημα του διακριτού λογαρίθμου σε ελλειπτικές καμπύλες.

Α. Διαδικασία Παραγωγής Υπογραφής

Για να υπογράψει ένα μήνυμα m (το hash της συναλλαγής), ο χρήστης με ιδιωτικό κλειδί dA επιλέγει έναν τυχαίο αριθμό k (nonce) από το διάστημα $[1, n-1]$ και εκτελεί τα εξής βήματα:

1. Υπολογίζει το σημείο $P = k \times G = (x1, y1)$ στην καμπύλη.
2. Θέτει $r = x1 \ (mod\ n)$. Αν $r = 0$, επιλέγει νέο k.
3. Υπολογίζει το $s = k^{-1}\ (z + r \times dA)\ (mod\ n)$, όπου z είναι το hash του μηνύματος.
4. Η τελική υπογραφή είναι το ζεύγος (r, s).

Β. Το Πρόβλημα του Τυχαίου Nonce (k)

Σύμφωνα με τους Brengel & Rossow (2021), η "Αχίλλειος πτέρνα" του ECDSA είναι η εξάρτησή του από την ποιότητα της γεννήτριας τυχαίων αριθμών (RNG) για την επιλογή του k. Εάν ο ίδιος αριθμός k χρησιμοποιηθεί σε δύο διαφορετικές συναλλαγές με το ίδιο ιδιωτικό κλειδί, τότε ένας επιτιθέμενος μπορεί να ανακτήσει το ιδιωτικό κλειδί dA μέσω απλών αλγεβρικών πράξεων, οδηγώντας σε ολική απώλεια κεφαλαίων. Για την αντιμετώπιση αυτού του κινδύνου, σύγχρονες υλοποιήσεις χρησιμοποιούν τον Ντετερμινιστικό ECDSA (RFC 6979), όπου το k παράγεται ως hash του μηνύματος και του κλειδιού, εξαλείφοντας τον παράγοντα τύχης [32].

4.4.2 Υπογραφές Schnorr: Η Εξέλιξη της Συναίνεσης: Οι υπογραφές Schnorr, οι οποίες ενσωματώθηκαν στο Bitcoin με την αναβάθμιση Taproot (BIP-340) τον Νοέμβριο του 2021, θεωρούνται ανώτερες του ECDSA λόγω της μαθηματικής τους απλότητας και της ιδιότητας της γραμμικότητας.

Α. Μαθηματική Δομή

Η εξίσωση παραγωγής υπογραφής Schnorr είναι:

$$s = k + e \times dA \ (mod\ n)$$

Όπου s η υπογραφή, k το nonce, e το hash του μηνύματος και dA το ιδιωτικό κλειδί.

Η διαδικασία επαλήθευσης ελέγχει αν:

$$s \times G = R + e \times PA$$

Η απλότητα αυτής της εξίσωσης (σε αντίθεση με την πολυπλοκότητα του ECDSA που απαιτεί αντιστροφή k^{-1} επιτρέπει ταχύτερη εκτέλεση.

Β. Γραμμικότητα και Συσσωμάτωση Κλειδιών (Key Aggregation)

Το σημαντικότερο πλεονέκτημα, όπως αναλύεται από τους Wu et al. (2022), είναι η ιδιότητα της γραμμικότητας. Εάν έχουμε πολλούς χρήστες που θέλουν να υπογράψουν μια κοινή συναλλαγή (Multi-Signature), μπορούμε να αθροίσουμε τα κλειδιά τους και τις υπογραφές τους:

$$\sum s_i = \sum k_i + e \times \sum d_{Ai}$$

Αυτό οδηγεί στην τεχνική MuSig (Multi-Signature Aggregation). Αντί να αποθηκεύουμε 10 ξεχωριστές υπογραφές στο Blockchain (σπαταλώντας χώρο και αυξάνοντας τα τέλη), αποθηκεύουμε μία και μοναδική "συσσωματωμένη" υπογραφή.

- Οφέλη Ιδιωτικότητας: Μια συναλλαγή πολλών ατόμων (MultiSig) φαίνεται εξωτερικά πανομοιότυπη με μια απλή συναλλαγή ενός ατόμου, δυσχεραίνοντας την ανάλυση της αλυσίδας (Chain Analysis).
- Οφέλη Επεκτασιμότητας: Μείωση του μεγέθους δεδομένων κατά 15-20% σε σύνθετες συναλλαγές [21].

Γ. Μαζική Επαλήθευση (Batch Verification)

Οι υπογραφές Schnorr επιτρέπουν στους κόμβους να επαληθεύουν όλες τις υπογραφές ενός μπλοκ ταυτόχρονα, αντί μία προς μία. Αυτό μειώνει δραστικά τον χρόνο που απαιτείται για τον συγχρονισμό ενός νέου κόμβου (IBD - Initial Block Download).

4.4.3 Ο Αλγόριθμος EdDSA (Edwards-curve Digital Signature Algorithm): Για δίκτυα υψηλής απόδοσης όπως το Solana και το Cardano, έχει επιλεγεί ο αλγόριθμος EdDSA στην καμπύλη Ed25519 (Twisted Edwards Curve).

Σύμφωνα με τους Zhang et al. (2020), το EdDSA προσφέρει δύο βασικά πλεονεκτήματα έναντι του secp256k1 (Bitcoin/Ethereum):

1. Ταχύτητα: Είναι σχεδιασμένο για να εκτελείται εξαιρετικά γρήγορα σε κοινούς επεξεργαστές, χωρίς να απαιτεί εξειδικευμένο υλικό.
2. Ασφάλεια: Είναι εγγενώς απρόσβλητο σε επιθέσεις "Side-Channel" (όπου ο επιτιθέμενος μετρά την κατανάλωση ρεύματος ή τον χρόνο εκτέλεσης για να βρει το κλειδί), καθώς οι πράξεις εκτελούνται σε σταθερό χρόνο (constant-time execution) ανεξαρτήτως των δεδομένων εισόδου [20].

4.4.4 Συγκριτική Επισκόπηση Αλγορίθμων: Η επιλογή του αλγορίθμου υπογραφής καθορίζει τις δυνατότητες του δικτύου.

Ο ECDSA (Bitcoin Legacy, Ethereum) είναι δοκιμασμένος και ευρέως διαδεδομένος, αλλά υποφέρει από το πρόβλημα της πλαστικότητας (malleability) και την έλλειψη γραμμικότητας. Οι υπογραφές είναι μεγάλες (71-72 bytes).

Ο Schnorr (Bitcoin Taproot) προσφέρει γραμμικότητα, ιδιωτικότητα μέσω aggregation και σταθερό μικρότερο μέγεθος (64 bytes), αλλά είναι νεότερη τεχνολογία με λιγότερες βιβλιοθήκες λογισμικού.

Ο EdDSA (Solana, Polkadot, Cardano) προσφέρει τη μέγιστη ταχύτητα και ασφάλεια σε επίπεδο υλοποίησης, αλλά δεν είναι συμβατός με τις καμπύλες του Bitcoin/Ethereum, δυσκολεύοντας τη διαλειτουργικότητα.

4.5 Διαχείριση Κλειδιών και Πρότυπα BIP (Bitcoin Improvement Proposals)

Η ασφάλεια των κρυπτονομισμάτων δεν εξαρτάται μόνο από την ανθεκτικότητα των αλγορίθμων κρυπτογράφησης, αλλά πρωτίστως από τον ασφαλή τρόπο δημιουργίας, αποθήκευσης και ανάκτησης των ιδιωτικών κλειδιών. Στα πρώτα χρόνια του Bitcoin, τα ψηφιακά πορτοφόλια (Wallets) ήταν "Μη-Ντετερμινιστικά" (JBOK - Just a Bunch Of Keys), δημιουργώντας τυχαία ζεύγη κλειδιών για κάθε συναλλαγή. Αυτό καθιστούσε τη δημιουργία αντιγράφων ασφαλείας (backup) εφιαλτική, καθώς ο χρήστης έπρεπε να αποθηκεύει συνεχώς νέα αρχεία.

Η λύση δόθηκε μέσω μιας σειράς Προτάσεων Βελτίωσης του Bitcoin (BIPs), οι οποίες υιοθετήθηκαν από τη συντριπτική πλειοψηφία των κρυπτονομισμάτων, δημιουργώντας τα πρότυπα της βιομηχανίας.

4.5.1 Ιεραρχικά Ντετερμινιστικά Πορτοφόλια (HD Wallets - BIP 32): Το πρότυπο BIP-32 εισήγαγε την έννοια των Ιεραρχικών Ντετερμινιστικών πορτοφολιών. Σε αυτό το σύστημα, όλα τα κλειδιά προέρχονται μαθηματικά από έναν μοναδικό "κύριο σπόρο" (Master Seed), συνήθως μεγέθους 128 έως 256 bits.

Η διαδικασία παραγωγής βασίζεται στη χρήση της συνάρτησης HMAC-SHA512. Ο σπόρος εισάγεται στη συνάρτηση και παράγει μια έξοδο 512 bits, η οποία χωρίζεται σε δύο μέρη:

- Αριστερά 256 bits: Αποτελούν το Κύριο Ιδιωτικό Κλειδί (Master Private Key - m).
- Δεξιά 256 bits: Αποτελούν τον Κύριο Κωδικό Αλυσίδας (Master Chain Code – c).

Ο συνδυασμός του κλειδιού και του κωδικού αλυσίδας ονομάζεται Εκτεταμένο Κλειδί (Extended Key). Χρησιμοποιώντας αυτό το ζεύγος, το πορτοφόλι μπορεί να παράγει μια δενδρική δομή "κλειδιών-παιδιών" (child keys) και "κλειδιών-εγγονιών", σε άπειρο βάθος.

Σύμφωνα με τους Dasgupta et al. (2021), το κύριο πλεονέκτημα αυτής της αρχιτεκτονικής είναι ότι επιτρέπει τον διαχωρισμό αρμοδιοτήτων: ένας οργανισμός μπορεί να χρησιμοποιήσει το *Εκτεταμένο Δημόσιο Κλειδί (xPub)* για να δημιουργεί διευθύνσεις είσπραξης σε έναν web server (χωρίς ρίσκο κλοπής), ενώ κρατά το *Εκτεταμένο Ιδιωτικό Κλειδί (xPriv)* σε αποθήκευση offline (Cold Storage) για την υπογραφή συναλλαγών [22].

4.5.2 Μνημονικές Φράσεις και Εντροπία (BIP-39): Το πρότυπο BIP-39 έλυσε το πρόβλημα της ανθρώπινης μνήμης. Οι χρήστες δυσκολεύονται να απομνημονεύσουν ή να αντιγράψουν χωρίς λάθη μια δεκαεξαδική σειρά 64 χαρακτήρων. Το BIP-39 τυποποιεί τη μετατροπή της αρχικής εντροπίας (του σπόρου) σε μια ακολουθία φυσικών λέξεων.

Η διαδικασία έχει ως εξής:

1. Παράγεται μια τυχαία ακολουθία εντροπίας (π.χ. 128 bits).
2. Υπολογίζεται ένα checksum (τα πρώτα bits του SHA-256 hash της εντροπίας) και προστίθεται στο τέλος.
3. Η συνολική ακολουθία χωρίζεται σε τμήματα των 11 bits.
4. Κάθε τμήμα 11 bits αντιστοιχεί σε έναν αριθμό από το 0 έως το 2047, ο οποίος λειτουργεί ως δείκτης σε μια προκαθορισμένη λίστα 2048 λέξεων (English Wordlist).

Έτσι προκύπτει η γνωστή "Φράση Ανάκτησης" (Seed Phrase) των 12 ή 24 λέξεων (π.χ. *army, van, defense, carry...*). Η γνώση αυτής της φράσης είναι μαθηματικά ισοδύναμη με την κατοχή όλων των χρημάτων του πορτοφολιού.

4.5.3 Ιεραρχία Πολλαπλών Νομισμάτων (BIP-44): Για την περαιτέρω οργάνωση των κλειδιών, το πρότυπο BIP-44 καθορίζει μια συγκεκριμένη δομή για τα "μονοπάτια παραγωγής" (derivation paths).

Ένα τυπικό μονοπάτι έχει τη μορφή:

m / 44' / coin_type' / account' / change / address_index

Όπου:

- 44': Δηλώνει ότι ακολουθείται το πρότυπο BIP-44.
- coin_type': Καθορίζει το κρυπτονόμισμα (π.χ. 0' για Bitcoin, 60' για Ethereum).
- account': Επιτρέπει στον χρήστη να έχει πολλαπλούς λογαριασμούς (π.χ. "Ταμιευτήριο", "Εξοδα").
- change: Διαχωρίζει τις διευθύνσεις που δίνονται σε τρίτους (External - 0) από τις διευθύνσεις για τα ρέστα (Internal - 1).

Αυτή η τυποποίηση επιτρέπει σε ένα μόνο λογισμικό πορτοφολιού (π.χ. Ledger, MetaMask) να διαχειρίζεται εκατοντάδες διαφορετικά κρυπτονομίσματα χρησιμοποιώντας τον ίδιο αρχικό σπόρο [22].

4.6 Προηγμένες Τεχνικές Ιδιωτικότητας και Ανωνυμίας

Ενώ η ψευδωνυμία του Bitcoin προσφέρει ένα βασικό επίπεδο κάλυψης, η σύγχρονη ανάλυση της αλυσίδας (Chain Analysis) επιτρέπει συχνά τη συσχέτιση διευθύνσεων με φυσικά πρόσωπα. Για την επίτευξη πραγματικής ανωνυμίας και τη συμμόρφωση με κανονισμούς προστασίας δεδομένων (όπως το GDPR), έχουν αναπτυχθεί προηγμένα κρυπτογραφικά πρωτόκολλα.

4.6.1 Αποδείξεις Μηδενικής Γνώσης (Zero-Knowledge Proofs - ZKP): Τα ZKPs αποτελούν μια επαναστατική μέθοδο στην κρυπτογραφία, επιτρέποντας σε ένα μέρος (Prover) να αποδείξει σε ένα άλλο μέρος (Verifier) την εγκυρότητα μιας πρότασης, χωρίς να αποκαλύψει καμία

επιπλέον πληροφορία πέραν του ότι η πρόταση είναι αληθής. Σύμφωνα με τους Ben-Sasson et al. (2020), ένα πρωτόκολλο ZKP πρέπει να ικανοποιεί τρεις αυστηρές ιδιότητες:

1. Πληρότητα (Completeness): Εάν η δήλωση είναι αληθής, ένας τίμιος Prover θα πείσει σίγουρα τον Verifier.
2. Ορθότητα (Soundness): Εάν η δήλωση είναι ψευδής, είναι στατιστικά αδύνατο για έναν κακόβουλο Prover να ξεγελάσει τον Verifier (εκτός από μια αμελητέα πιθανότητα).
3. Μηδενική Γνώση (Zero-Knowledge): Μετά το πέρας της διαδικασίας, ο Verifier δεν γνωρίζει τίποτα περισσότερο από το γεγονός ότι η δήλωση είναι αληθής [23].

4.6.2 zk-SNARKs vs zk-STARKs: Η έρευνα έχει οδηγήσει σε δύο κύριες υλοποιήσεις ZKP, με διαφορετικά χαρακτηριστικά ασφαλείας και απόδοσης:

- zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge): Χρησιμοποιούνται ευρέως (π.χ. στο Zcash και στο Ethereum Layer 2). Το κύριο χαρακτηριστικό τους είναι το εξαιρετικά μικρό μέγεθος της απόδειξης (μόλις μερικά bytes) και η ταχύτατη επαλήθευση (milliseconds). Ωστόσο, έχουν ένα σημαντικό μειονέκτημα: απαιτούν μια διαδικασία "Trusted Setup" για τη δημιουργία των αρχικών παραμέτρων. Εάν τα μυστικά κλειδιά αυτής της διαδικασίας διαρεύσουν, μπορεί να δημιουργηθούν πλαστά νομίσματα (αν και δεν μπορεί να παραβιαστεί η ιδιωτικότητα).
- zk-STARKs (Zero-Knowledge Scalable Transparent Argument of Knowledge): Θεωρούνται η εξέλιξη των SNARKs. Το βασικό τους πλεονέκτημα είναι η Διαφάνεια (Transparency), καθώς δεν απαιτούν Trusted Setup, εξαλείφοντας τον κίνδυνο κερκόπορτας. Επιπλέον, βασίζονται σε συναρτήσεις κατακερματισμού και όχι σε ελλειπτικές καμπύλες, γεγονός που τα καθιστά ανθεκτικά σε κβαντικούς υπολογιστές (Post-Quantum Secure). Το μειονέκτημά τους είναι ότι παράγουν μεγαλύτερες αποδείξεις σε μέγεθος, απαιτώντας περισσότερο χώρο αποθήκευσης [24].

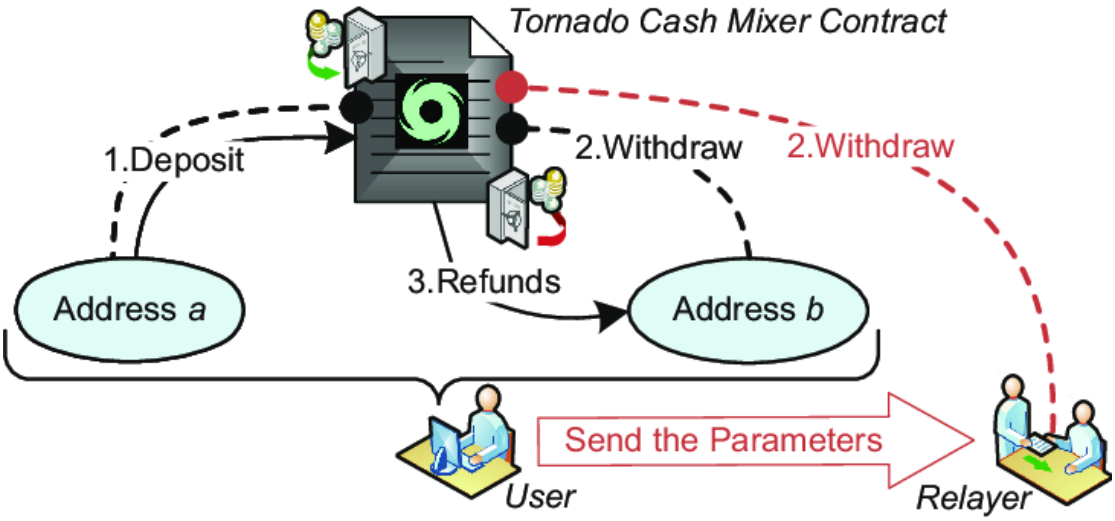
4.6.3 Υπογραφές Δακτυλίου (Ring Signatures): Μια διαφορετική προσέγγιση εφαρμόζεται στο κρυπτονόμισμα Monero. Αντί να αποκρύπτει τα δεδομένα με ZKPs, χρησιμοποιεί την τεχνική της "απόκρυψης μέσα στο πλήθος". Όταν ένας χρήστης υπογράφει μια συναλλαγή, η ψηφιακή του υπογραφή αναμιγνύεται μαθηματικά με υπογραφές παλαιότερων συναλλαγών που επιλέγονται τυχαία από το Blockchain (Decoys). Για έναν εξωτερικό παρατηρητή, είναι υπολογιστικά αδύνατο να διακρίνει ποια από τις υπογραφές του "δακτυλίου" ανήκει στον πραγματικό αποστολέα. Αυτό εξασφαλίζει την "αδυναμία σύνδεσης" (unlinkability) των συναλλαγών.

4.6.4 Εμπιστευτικές Συναλλαγές (Confidential Transactions - RingCT): Σε συνδυασμό με τις υπογραφές δακτυλίου, χρησιμοποιείται το πρωτόκολλο RingCT για την απόκρυψη των ποσών. Χρησιμοποιώντας μια κρυπτογραφική δέσμευση (Pedersen Commitment), ο αποστολέας δεσμεύει το ποσό της συναλλαγής χωρίς να το αποκαλύψει. Το δίκτυο μπορεί να επιβεβαιώσει ότι *Είσοδοι = Έξοδοι* (άρα δεν δημιουργήθηκε νέο χρήμα από το πουθενά), χωρίς όμως να γνωρίζει ποιο είναι το ακριβές νούμερο που μεταφέρθηκε.

4.6.5 Υπηρεσίες Ανάμειξης (Mixers και Tumblers): Παρά την ψευδωνυμία που προσφέρουν τα δημόσια δίκτυα όπως το Bitcoin, η ανάλυση της αλυσίδας (Chain Analysis) από εξειδικευμένες εταιρείες μπορεί να συνδέσει τις διευθύνσεις με φυσικά πρόσωπα, παρακολουθώντας τη ροή των νομισμάτων. Για την αντιμετώπιση αυτού του προβλήματος και την αποκοπή της σύνδεσης μεταξύ αποστολέα και παραλήπτη, αναπτύχθηκαν οι Υπηρεσίες Ανάμειξης (Mixers ή Tumblers).

Η βασική αρχή λειτουργίας ενός Mixer είναι η συγκέντρωση κεφαλαίων από πολλούς διαφορετικούς χρήστες σε μια κοινή δεξαμενή. Στη συνέχεια, το σύστημα ανακατεύει τα νομίσματα και τα επιστρέφει στους χρήστες σε νέες διευθύνσεις, καθιστώντας εξαιρετικά δύσκολο τον εντοπισμό της αρχικής πηγής. Η βιβλιογραφία διακρίνει τις υπηρεσίες αυτές σε τρεις κατηγορίες:

- Κεντρικοποιημένα Mixers: Ο χρήστης στέλνει τα νομίσματά του σε μια κεντρική πλατφόρμα, η οποία αναλαμβάνει την ανάμειξη. Αυτό το μοντέλο ενέχει τεράστιο κίνδυνο αντισυμβαλλομένου (Custodial Risk), καθώς ο διαχειριστής μπορεί να κλέψει τα κεφάλαια ή να διατηρήσει αρχεία καταγραφής (logs) που αποκαλύπτουν τις ταυτότητες των χρηστών.
- Αποκεντρωμένα Mixers (CoinJoin): Πρόκειται για ένα πρωτόκολλο (χρησιμοποιείται κυρίως σε πορτοφόλια όπως το Wasabi και το Samourai), όπου πολλοί χρήστες συνυπογράφουν συνεργατικά μια ενιαία συναλλαγή. Στην έξοδο της συναλλαγής, τα νομίσματα διανέμονται σε όλους τους συμμετέχοντες σε ίσα ποσά, καθιστώντας αδύνατη τη μαθηματική ταύτιση εισόδων και εξόδων. Το μοντέλο αυτό είναι μη-εμπιστευτικό (non-custodial), καθώς οι χρήστες δεν παραδίδουν ποτέ τον έλεγχο των ιδιωτικών τους κλειδιών.
- Mixers Έξυπνων Συμβολαίων (π.χ. Tornado Cash): Στο οικοσύστημα του Ethereum, η ανάμειξη επιτυγχάνεται μέσω Έξυπνων Συμβολαίων σε συνδυασμό με Αποδείξεις Μηδενικής Γνώσης (zk-SNARKs). Ο χρήστης καταθέτει ETH στο συμβόλαιο και λαμβάνει ένα κρυπτογραφικό αποδεικτικό. Αργότερα, χρησιμοποιεί αυτό το αποδεικτικό για να κάνει ανάληψη από μια εντελώς νέα διεύθυνση, με το δίκτυο να επιβεβαιώνει την εγκυρότητα της κατάθεσης χωρίς να αποκαλύπτει ποια ακριβώς ήταν.



Εικόνα 4.1: Διαγραμματική απεικόνιση της λειτουργίας του πρωτοκόλλου ανάμειξης Tornado Cash και του ρόλου του Αναμεταδότη (Relayer).

4.6.6 Υπολογισμός Πολλαπλών Μερών (Multi-Party Computation - MPC): Η διαχείριση των ιδιωτικών κλειδιών αποτελεί το μεγαλύτερο σημείο ευπάθειας (Single Point of Failure) στα δίκτυα Blockchain. Αν το ιδιωτικό κλειδί χαθεί ή κλαπεί, η πρόσβαση στα κεφάλαια χάνεται οριστικά. Το Ασφαλές Πρωτόκολλο Υπολογισμού Πολλαπλών Μερών (Secure Multi-Party Computation - sMPC) προσφέρει μια κρυπτογραφική λύση σε αυτό το πρόβλημα, προστατεύοντας ταυτόχρονα την ιδιωτικότητα.

Το MPC είναι ένας κλάδος της κρυπτογραφίας που επιτρέπει σε πολλά μέρη να υπολογίσουν από κοινού μια συνάρτηση πάνω στα δεδομένα τους, διατηρώντας τα ίδια τα δεδομένα απόλυτα μυστικά. Στο πλαίσιο των κρυπτονομισμάτων, το MPC χρησιμοποιείται για τη δημιουργία Συστημάτων Υπογραφής Κατωφλίου (Threshold Signature Schemes - TSS).

Η διαδικασία λειτουργεί ως εξής:

1. Κατανεμημένη Παραγωγή: Το ιδιωτικό κλειδί δεν δημιουργείται ποτέ ολόκληρο σε μία συσκευή. Αντίθετα, δημιουργείται σε "κομμάτια" (key shares) τα οποία μοιράζονται σε διαφορετικούς υπολογιστές/κόμβους.
2. Συνεργατική Υπογραφή: Για να εγκριθεί μια συναλλαγή, απαιτείται η συμμετοχή ενός ελάχιστου αριθμού κόμβων (π.χ. 3 από τους 5). Αυτοί οι κόμβοι χρησιμοποιούν τα κομμάτια τους για να υπογράψουν τη συναλλαγή συνεργατικά, χωρίς να χρειάζεται να τα ενώσουν ποτέ.

Πλεονεκτήματα του MPC έναντι των παραδοσιακών Multi-Sig:

- Ιδιωτικότητα: Σε ένα παραδοσιακό Multi-Sig (Πολλαπλών Υπογραφών), η δομή του συμβολαίου (π.χ. ότι είναι 3-από-5) και οι υπογραφές όλων των συμμετεχόντων καταγράφονται δημόσια στο Blockchain. Αντίθετα, το MPC δημιουργεί μία, τυπική και μοναδική ψηφιακή υπογραφή (π.χ. ECDSA ή EdDSA). Για έναν εξωτερικό παρατηρητή, η συναλλαγή φαίνεται σαν να προήλθε από έναν μόνο χρήστη.
- Εξοικονόμηση Κόστους (Gas Fees): Επειδή το δίκτυο βλέπει και επικυρώνει μόνο μία υπογραφή (αντί για πολλές), το μέγεθος της συναλλαγής παραμένει μικρό, μειώνοντας δραματικά τα τέλη δικτύου στο Ethereum.
- Ευελιξία: Στο MPC, οι διαχειριστές μπορούν να αλλάξουν τον αριθμό των συμμετεχόντων (π.χ. από 3-από-5 σε 4-από-7) εκτός αλυσίδας (off-chain), χωρίς να χρειάζεται να μεταφέρουν τα κεφάλαια σε νέα διεύθυνση, κάτι που είναι υποχρεωτικό στα παραδοσιακά Multi-Sig.

4.7 Η Απειλή των Κβαντικών Υπολογιστών και η Μετα-Κβαντική Εποχή

Η ασφάλεια όλων των σύγχρονων κρυπτονομισμάτων (Bitcoin, Ethereum, κ.λπ.) βασίζεται στην υπόθεση ότι ορισμένα μαθηματικά προβλήματα (όπως η παραγοντοποίηση μεγάλων αριθμών στον RSA ή ο διακριτός λογάριθμος στην ECC) είναι πρακτικά άλυτα για τους κλασικούς υπολογιστές. Ωστόσο, η ραγδαία εξέλιξη της κβαντικής πληροφορικής απειλεί να καταρρίψει αυτό το αξίωμα.

4.7.1 Η Φύση της Απειλής: Shor και Grover Σύμφωνα με τους Fernandez-Carames & Fraga-Lamas (2020), οι κβαντικοί υπολογιστές εκμεταλλεύονται φαινόμενα της κβαντομηχανικής

(υπέρθεση και διεμπλοκή) για να εκτελέσουν υπολογισμούς με εκθετικά μεγαλύτερη ταχύτητα από τους συμβατικούς. Η απειλή για το Blockchain προέρχεται κυρίως από δύο αλγορίθμους:

1. Αλγόριθμος του Shor: Είναι ο πιο καταστροφικός. Μπορεί να βρει το ιδιωτικό κλειδί από το δημόσιο κλειδί σε πολυωνυμικό χρόνο. Αυτό σημαίνει ότι τα συστήματα RSA και ECC (secp256k1) θα καταρρεύσουν πλήρως. Ένας επιτιθέμενος με επαρκώς ισχυρό κβαντικό υπολογιστή θα μπορούσε να υπολογίσει τα ιδιωτικά κλειδιά όλων των διευθύνσεων που έχουν εκθέσει το δημόσιο κλειδί τους στο δίκτυο και να αδειάσει τα πορτοφόλια τους [25].
2. Αλγόριθμος του Grover: Αφορά τις συμμετρικές κρυπτογραφικές συναρτήσεις και το Hashing (SHA-256). Ο αλγόριθμος αυτός προσφέρει τετραγωνική επιτάχυνση στην αναζήτηση αδόμητων δεδομένων. Πρακτικά, αυτό σημαίνει ότι μειώνει την ασφάλεια ενός hash στο μισό (π.χ. το SHA-256 γίνεται ισοδύναμο με SHA-128). Ωστόσο, αυτή η απειλή είναι διαχειρίσιμη, καθώς αρκεί απλώς η αύξηση του μεγέθους των hashes (π.χ. μετάβαση σε SHA-512) για να αντισταθμιστεί [24].

4.7.2 Υποψήφιοι Αλγόριθμοι PQC (NIST Standardization): Για την αντιμετώπιση του αλγορίθμου Shor, η επιστημονική κοινότητα, υπό την αιγίδα του NIST, έχει αναπτύξει νέες οικογένειες αλγορίθμων που βασίζονται σε μαθηματικά προβλήματα τα οποία οι κβαντικοί υπολογιστές *δεν* μπορούν να λύσουν αποδοτικά. Οι κυριότερες κατηγορίες είναι:

- Κρυπτογραφία Πλεγμάτων (Lattice-based Cryptography): Θεωρείται η πιο υποσχόμενη λύση. Βασίζεται στη δυσκολία εύρεσης του κοντινότερου διανύσματος σε ένα πλέγμα πολλών διαστάσεων (Shortest Vector Problem). Οι αλγόριθμοι CRYSTALS-Kyber (για κρυπτογράφηση) και CRYSTALS-Dilithium (για ψηφιακές υπογραφές) έχουν επιλεγεί ως πρότυπα. Προσφέρουν ισορροπία μεταξύ μεγέθους κλειδιού και ταχύτητας, αλλά τα κλειδιά τους παραμένουν σημαντικά μεγαλύτερα από αυτά της ECC.
- Υπογραφές βασισμένες σε Hash (Hash-based Signatures): Χρησιμοποιούν δέντρα Merkle για τη δημιουργία υπογραφών (π.χ. SPHINCS+, XMSS). Είναι εξαιρετικά ασφαλείς και κατανοητές, αλλά παράγουν πολύ μεγάλες υπογραφές (δεκάδες Kilobytes), γεγονός που θα επιβάρυνε σημαντικά το μέγεθος του Blockchain (bloating).
- Πολυωνυμική Κρυπτογραφία (Multivariate Cryptography): Βασίζεται στην επίλυση συστημάτων πολυωνυμικών εξισώσεων. Αν και προσφέρει πολύ μικρές υπογραφές, τα δημόσια κλειδιά είναι τεράστια [26].

4.7.3 Προκλήσεις Μετάβασης και Κρυπτο-Ευελιξία (Crypto-Agility): Η μετάβαση σε PQC πρότυπα δεν είναι απλή υπόθεση "αναβάθμισης λογισμικού". Οι Rehman et al. (2021) επισημαίνουν ότι τα νέα κλειδιά και υπογραφές είναι πολύ μεγαλύτερα σε μέγεθος, κάτι που θα μείωνε δραματικά την ταχύτητα συναλλαγών (TPS) και θα αύξανε το κόστος αποθήκευσης. Η προτεινόμενη στρατηγική είναι η Κρυπτο-Ευελιξία: Ο σχεδιασμός των πρωτοκόλλων ώστε να υποστηρίζουν πολλαπλούς αλγορίθμους ταυτόχρονα. Για παράδειγμα, το Bitcoin θα μπορούσε να εισάγει νέους τύπους διευθύνσεων PQC μέσω ενός Soft Fork. Οι χρήστες θα πρέπει να μεταφέρουν τα κεφάλαιά τους από τις παλιές διευθύνσεις (Legacy ECC) στις νέες (Quantum-Resistant) πριν οι κβαντικοί υπολογιστές γίνουν πρακτικά διαθέσιμοι. Τα "χαμένα" νομίσματα (Satoshi's coins) που δεν θα μετακινηθούν, θα κινδυνεύσουν να κλαπούν [27].

ΚΕΦΑΛΑΙΟ 5: ΜΗΧΑΝΙΣΜΟΙ ΣΥΝΑΙΝΕΣΗΣ (CONSENSUS PROTOCOLS)

5.1 Θεωρητικό Υπόβαθρο:

Το Πρόβλημα των Βυζαντινών Στρατηγών και οι Ιδιότητες Ορθότητας

Η επίτευξη συμφωνίας (consensus) σε ένα κατανεμημένο σύστημα αποτελεί ένα από τα παλαιότερα και πιο σύνθετα προβλήματα της πληροφορικής. Σε αντίθεση με τα κεντρικοποιημένα συστήματα, όπου η "αλήθεια" ορίζεται από μια κεντρική βάση δεδομένων (Master Node), στα δίκτυα Blockchain κάθε κόμβος διατηρεί το δικό του αυτόνομο αντίγραφο του καθολικού. Το θεμελιώδες ερώτημα που προκύπτει είναι: *Πώς εξασφαλίζουμε ότι όλοι οι κόμβοι συμφωνούν στην ίδια ακριβώς κατάσταση (state) του δικτύου, όταν ορισμένοι από αυτούς μπορεί να είναι ελαττωματικοί, εκτός σύνδεσης ή ακόμα και κακόβουλοι;*

Το πρόβλημα αυτό περιγράφεται αλληγορικά ως το Πρόβλημα των Βυζαντινών Στρατηγών (Byzantine Generals Problem). Φανταστείτε μια ομάδα στρατηγών που πολιορκούν μια πόλη και πρέπει να αποφασίσουν συντονισμένα αν θα επιτεθούν ή θα υποχωρήσουν. Η επικοινωνία γίνεται μόνο μέσω αγγελιοφόρων σε ένα εχθρικό περιβάλλον. Αν οι στρατηγοί δεν συντονιστούν (π.χ. αν οι μισοί επιτεθούν και οι άλλοι μισοί υποχωρήσουν), θα ηττηθούν. Το πρόβλημα επιδεινώνεται δραματικά αν υπάρχουν "προδότες" στρατηγοί που στέλνουν σκόπιμα αντικρουόμενα μηνύματα για να προκαλέσουν σύγχυση. Σύμφωνα με την ανάλυση των Xiao et al. (2020), ένα πρωτόκολλο συναίνεσης σε Blockchain πρέπει να είναι Byzantine Fault Tolerant (BFT), δηλαδή να διαθέτει μαθηματικές εγγυήσεις ότι το δίκτυο θα συνεχίσει να λειτουργεί σωστά ακόμα και αν έως το 1/3 των κόμβων ενεργεί κακόβουλα [7].

5.1.1 Η Ιδιότητα της Ασφάλειας (Safety Property): Στη θεωρία κατανεμημένων συστημάτων, η Ασφάλεια ορίζεται με τη φράση *"Τίποτα κακό δεν θα συμβεί ποτέ"* (Bad things never happen). Στο πλαίσιο του Blockchain, αυτό μεταφράζεται στην εγγύηση της Μοναδικότητας του Ιστορικού. Συγκεκριμένα, ένα ασφαλές πρωτόκολλο εγγυάται ότι:

- Δύο ειλικρινείς κόμβοι δεν θα επικυρώσουν ποτέ δύο διαφορετικά μπλοκ στο ίδιο ύψος της αλυσίδας (αποφυγή μόνιμων forks).
- Μια επικυρωμένη συναλλαγή δεν μπορεί να ανακληθεί ή να τροποποιηθεί. Αυτό οδηγεί στην έννοια της Οριστικότητας (Finality).
    - Ντετερμινιστική Οριστικότητα: Υπάρχει σε αλγορίθμους τύπου BFT (π.χ. Cosmos/Tendermint). Μόλις ένα μπλοκ προστεθεί, είναι 100% τελικό.
    - Πιθανοτική Οριστικότητα: Υπάρχει στο Bitcoin (PoW). Ένα μπλοκ δεν είναι ποτέ 100% τελικό, αλλά όσο περνάει ο χρόνος και προστίθενται νέα μπλοκ, η πιθανότητα ανατροπής του τείνει ασυμπτωτικά στο μηδέν.

5.1.2 Η Ιδιότητα της Ζωντάνιας (Liveness Property): Η Ζωντάνια ορίζεται με τη φράση "Κάτι καλό θα συμβεί τελικά" (Good things eventually happen). Αφορά την ικανότητα του συστήματος να παραμένει λειτουργικό και να επεξεργάζεται αιτήματα, ανεξάρτητα από τις συνθήκες του δικτύου. Στο Blockchain, η Ζωντάνια εγγυάται ότι:

- Κάθε έγκυρη συναλλαγή που υποβάλλεται στο δίκτυο θα συμπεριληφθεί τελικά σε κάποιο μπλοκ και θα εκτελεστεί (Guaranteed Termination).

- Το δίκτυο δεν θα "κολλήσει" (deadlock) ποτέ, ακόμη και αν μεγάλο μέρος των κόμβων αποσυνδεθεί. Η ιδιότητα αυτή είναι άμεσα συνδεδεμένη με την Αντίσταση στη Λογοκρισία (Censorship Resistance): εφόσον το δίκτυο είναι "ζωντανό", κανείς δεν μπορεί να εμποδίσει επ' αόριστον την εκτέλεση μιας έγκυρης συναλλαγής.

5.1.3 Το Δίλημμα FLP και οι Αρχιτεκτονικές Επιλογές: Σύμφωνα με το θεμελιώδες Θεώρημα Αδυναμίας των FLP (Fischer, Lynch, Paterson Impossibility Result), σε ένα πλήρως ασύγχρονο δίκτυο (όπου δεν υπάρχουν εγγυήσεις για τον χρόνο παράδοσης μηνυμάτων, όπως το Internet), είναι μαθηματικά αδύνατο να σχεδιαστεί ένας αλγόριθμος συναίνεσης που να εγγυάται ταυτόχρονα και την Ασφάλεια και τη Ζωντάνια, παρουσία έστω και ενός ελαττωματικού κόμβου. Ως εκ τούτου, κάθε Blockchain αναγκάζεται να κάνει μια αρχιτεκτονική επιλογή (trade-off):

1. Προτεραιότητα στη Ζωντάνια (Nakamoto Consensus - Bitcoin/Ethereum 1.0): Το δίκτυο δεν σταματά ποτέ. Αν υπάρξει διαφωνία ή διαχωρισμός του δικτύου (partition), το σύστημα επιτρέπει τη δημιουργία προσωρινών διακλαδώσεων (forks), θυσιάζοντας στιγμιαία την Ασφάλεια για να διασφαλίσει ότι οι συναλλαγές συνεχίζουν να ρέουν. Η Ασφάλεια επιτυγχάνεται τελικά ("Eventual Consistency").
2. Προτεραιότητα στην Ασφάλεια (Classic BFT - Hyperledger/Cosmos/Algorand): Εάν υπάρξει ασυμφωνία ή διαχωρισμός του δικτύου, το σύστημα σταματά να παράγει νέα μπλοκ (halt) μέχρι να αποκατασταθεί η επικοινωνία. Προτιμά να "παγώσει" παρά να επιτρέψει την ύπαρξη δύο διαφορετικών εκδοχών της αλήθειας [18].

5.2 Απόδειξη Εργασίας (Proof of Work - PoW)

Το Proof of Work (PoW) ήταν ο πρώτος μηχανισμός που έλυσε πρακτικά το πρόβλημα των Βυζαντινών Στρατηγών σε ανοιχτό δίκτυο. Εισήχθη από τον Satoshi Nakamoto και βασίζεται στην ιδέα ότι η παραγωγή ενός μπλοκ πρέπει να είναι υπολογιστικά δαπανηρή, αλλά η επαλήθευσή του τετριμμένη.

5.2.1 Η Μαθηματική Δομή της Εξόρυξης (Mining): Η διαδικασία της εξόρυξης συχνά παρεξηγείται ως "λύση πολύπλοκων μαθηματικών εξισώσεων". Στην πραγματικότητα, είναι μια διαδικασία επαναλαμβανόμενων δοκιμών (brute-force trial and error).

Ο miner κατασκευάζει ένα υποψήφιο μπλοκ B και αναζητά έναν τυχαίο αριθμό n (nonce) τέτοιο ώστε:

$$SHA256(SHA256(Header(B) + n)) \leq Target$$

Όπου Target είναι ένας αριθμός 256-bit που καθορίζει τη δυσκολία. Επειδή η έξοδος της SHA-256 είναι ψευδοτυχαία και ομοιόμορφα κατανεμημένη, δεν υπάρχει τρόπος πρόβλεψης του nonce. Ο miner πρέπει να δοκιμάζει δισεκατομμύρια συνδυασμούς ανά δευτερόλεπτο. Η πιθανότητα εύρεσης έγκυρου hash ακολουθεί την κατανομή Poisson.

5.2.2 Προσαρμογή Δυσκολίας και Χρονικοί Στόχοι: Για να διατηρηθεί σταθερός ο ρυθμός παραγωγής μπλοκ (block time), το πρωτόκολλο αναπροσαρμόζει δυναμικά τον στόχο. Στο Bitcoin, αυτό συμβαίνει κάθε 2016 μπλοκ (περίπου 2 εβδομάδες).

Ο τύπος προσαρμογής είναι:

$$New\ Target\ =\ Old\ Target\ \times \frac{Actual\ Time}{Expected\ Time}$$

Εάν η συνολική ισχύς (Hashrate) αυξηθεί, τα μπλοκ παράγονται πιο γρήγορα (Actual < Expected), άρα ο στόχος μικραίνει (γίνεται πιο δύσκολο να βρεθεί).

- Εάν η ισχύς μειωθεί, ο στόχος μεγαλώνει.

Οι Gai et al. (2020) αναλύουν πώς αυτός ο μηχανισμός προστατεύει το δίκτυο από τις εκθετικές αυξήσεις της υπολογιστικής ισχύος λόγω της εξέλιξης του hardware (Νόμος του Moore) [33].

5.2.3 Η Εξέλιξη του Υλικού Εξόρυξης και οι Σύγχρονες Προκλήσεις: Η ιστορία του Proof of Work χαρακτηρίζεται από έναν συνεχή και αμείλικτο αγώνα εξοπλισμών (hardware arms race). Στα πρώτα χρόνια του Bitcoin (2009-2010), η εξόρυξη ήταν εφικτή με απλούς κεντρικούς επεξεργαστές (CPU). Σύντομα, οι miners ανακάλυψαν ότι οι Κάρτες Γραφικών (GPU), λόγω της αρχιτεκτονικής τους που επιτρέπει χιλιάδες παράλληλους υπολογισμούς, ήταν εκθετικά πιο αποδοτικές. Το 2013 σηματοδότησε την είσοδο των FPGA (Field-Programmable Gate Arrays) και τελικά των ASIC (Application-Specific Integrated Circuits). Ένα σύγχρονο ASIC (π.χ. Antminer S19 Pro) είναι σχεδιασμένο σε επίπεδο πυριτίου αποκλειστικά για τον αλγόριθμο SHA-256 και είναι εκατομμύρια φορές πιο αποδοτικό από οποιονδήποτε γενικό υπολογιστή. Σύμφωνα με τους Gallersdörfer et al. (2020), αυτή η εξειδίκευση οδήγησε στη βιομηχανοποίηση της εξόρυξης, αποκλείοντας ουσιαστικά τους ερασιτέχνες χρήστες και δημιουργώντας ανησυχίες για κεντρικοποίηση, καθώς η παραγωγή των ASICs ελέγχεται από ελάχιστες εταιρείες (ολιγοπώλιο) [31].

Το Φαινόμενο του Cloud Mining και οι Κίνδυνοι Παράλληλα με την εξέλιξη του υλικού, αναπτύχθηκε το επιχειρηματικό μοντέλο της Εξόρυξης Νέφους (Cloud Mining). Αυτή η υπηρεσία επιτρέπει σε ιδιώτες επενδυτές να ενοικιάζουν επεξεργαστική ισχύ (Hashrate) από απομακρυσμένα κέντρα δεδομένων, χωρίς να χρειάζεται να αγοράσουν, να εγκαταστήσουν ή να συντηρήσουν τον φυσικό εξοπλισμό. Αν και αυτό μειώνει το τεχνικό εμπόδιο εισόδου, η ακαδημαϊκή έρευνα επισημαίνει σοβαρούς κινδύνους. Πρώτον, εισάγεται ο "κίνδυνος αντισυμβαλλομένου" (counterparty risk), καθώς πολλές πλατφόρμες Cloud Mining αποδείχθηκαν σχήματα Ponzi, όπου οι αποδόσεις των παλαιών επενδυτών πληρώνονταν από τα κεφάλαια των νέων. Δεύτερον, ακόμη και στις νόμιμες υπηρεσίες, προκύπτει ζήτημα κεντρικοποίησης της ψήφου: ενώ ο ενοικιαστής λαμβάνει την οικονομική ανταμοιβή, το δικαίωμα ψήφου (που αφορά αλλαγές στο πρωτόκολλο) παραμένει στον διαχειριστή του κέντρου δεδομένων, συγκεντρώνοντας έτσι επικίνδυνα μεγάλη ισχύ σε λίγες οντότητες.

Η Πίεση του ESG και η Στροφή στην Πράσινη Ενέργεια Επιπροσθέτως, η αυξανόμενη πίεση από θεσμικούς επενδυτές για συμμόρφωση με τα κριτήρια ESG (Environmental, Social, and Governance) έχει αναδιαμορφώσει δραστικά τη στρατηγική των εγκαταστάσεων εξόρυξης. Καθώς η κατανάλωση ενέργειας του Bitcoin δέχεται έντονη κριτική, παρατηρείται μια μαζική μετατόπιση προς τις Ανανεώσιμες Πηγές Ενέργειας (ΑΠΕ). Σύμφωνα με πρόσφατες μελέτες των Sedlmeir et al. (2020), οι miners αναζητούν πλέον "εγκλωβισμένη ενέργεια" (stranded energy) – δηλαδή πλεόνασμα ενέργειας που θα πήγαινε χαμένο, όπως υδροηλεκτρική ενέργεια σε απομακρυσμένες περιοχές ή φυσικό αέριο που καίγεται στις πετρελαιοπηγές (gas flaring). Με αυτόν τον τρόπο, το mining μετατρέπεται από περιβαλλοντικό βάρος σε εργαλείο εξισορρόπησης

του ηλεκτρικού δικτύου (grid balancing) και οικονομικής επιδότησης των πράσινων υποδομών, επιχειρώντας να αντιστρέψει το αρνητικό αφήγημα [30].

5.2.4 Δεξαμενές Εξόρυξης (Mining Pools): Λόγω της τεράστιας δυσκολίας, είναι στατιστικά αδύνατο για έναν μεμονωμένο miner να βρει ένα μπλοκ. Γι' αυτό, οι miners ενώνουν την ισχύ τους σε "Δεξαμενές" (Pools). Ο διαχειριστής του Pool μοιράζει την εργασία και, όταν βρεθεί ένα μπλοκ, διανέμει την ανταμοιβή στα μέλη αναλογικά με τη συνεισφορά τους. Ωστόσο, αυτό εισάγει κίνδυνο κεντρικοποίησης: αν 3-4 μεγάλα Pools συνεργαστούν, μπορούν θεωρητικά να ελέγξουν το 51% του δικτύου.

5.3 Απόδειξη Συμμετοχής (Proof of Stake - PoS)

Ως απάντηση στους ενεργειακούς και περιβαλλοντικούς περιορισμούς του PoW, αναπτύχθηκε ο μηχανισμός Proof of Stake (PoS). Η θεμελιώδης διαφορά έγκειται στην αντικατάσταση της "φυσικής ενέργειας" (ηλεκτρισμός) με "οικονομική ενέργεια" (κεφάλαιο). Στο PoS, η πιθανότητα ενός κόμβου να δημιουργήσει το επόμενο μπλοκ δεν εξαρτάται από την υπολογιστική του ισχύ, αλλά από το μερίδιο ιδιοκτησίας του στο δίκτυο.

5.3.1 Μηχανισμός Επιλογής Επικυρωτών (Validator Selection Strategies): Η διαδικασία επιλογής του δημιουργού μπλοκ (block proposer) πρέπει να είναι ψευδο-τυχαία, ώστε κανείς να μην μπορεί να προβλέψει με ακρίβεια ποιος θα είναι ο επόμενος (για να αποφευχθούν στοχευμένες επιθέσεις DDoS).

Σύμφωνα με τους Nguyen et al. (2020), υπάρχουν δύο κύριες στρατηγικές επιλογής στη βιβλιογραφία:

1. Επιλογή Βάσει Τυχαίας Κλήρωσης (Randomized Block Selection): Το σύστημα αναζητά έναν κόμβο που κατέχει τον συνδυασμό της χαμηλότερης τιμής hash και του μεγαλύτερου πονταρίσματος (stake). Ο τύπος είναι συνήθως:

$$Hash(Header + Public\,Key) \leq Target \times Balance$$

2. Επιλογή Βάσει Ηλικίας Νομίσματος (Coin Age Selection): Η πιθανότητα αυξάνεται όσο περισσότερο καιρό τα νομίσματα παραμένουν αχρησιμοποίητα. Η "ηλικία" ορίζεται ως $Coin\,Age = Amount \times Holding\,Period$. Μόλις ο κόμβος δημιουργήσει μπλοκ, η ηλικία των νομισμάτων του μηδενίζεται. Ωστόσο, αυτή η μέθοδος εγκαταλείφθηκε στα σύγχρονα δίκτυα (όπως το Ethereum) επειδή αποθάρρυνε τη συμμετοχή, ωθώντας τους χρήστες να κρατούν τα νομίσματά τους αδρανή [28].

5.3.2 Η Πρόκληση της Τυχαιότητας (Source of Randomness): Η παραγωγή αληθινής τυχαιότητας σε ένα ντετερμινιστικό σύστημα όπως το Blockchain είναι εξαιρετικά δύσκολη. Εάν οι validators μπορούν να προβλέψουν ή να επηρεάσουν την τυχαιότητα, μπορούν να χειραγωγήσουν την επιλογή του επόμενου νικητή (Grinding Attack).

Για την αντιμετώπιση αυτού, το Ethereum 2.0 χρησιμοποιεί τον μηχανισμό RANDAO σε συνδυασμό με κρυπτογραφικές υπογραφές BLS. Κάθε validator συνεισφέρει ένα κομμάτι "εντροπίας" (τυχαία δεδομένα) το οποίο αναμιγνύεται με τα υπόλοιπα, δημιουργώντας έναν απρόβλεπτο αριθμό που καθορίζει τους ηγέτες της επόμενης εποχής (epoch).

5.3.3 Οικονομικά Κίνητρα και Κυρώσεις (Rewards & Penalties): Η ασφάλεια του PoS είναι καθαρά κρυπτο-οικονομική. Βασίζεται στο αξίωμα ότι οι συμμετέχοντες είναι ορθολογικοί δρώντες που επιδιώκουν το κέρδος.

- Ανταμοιβές (Rewards): Οι validators λαμβάνουν τόκους (staking yield) και τα τέλη συναλλαγών για την τίμια συμμετοχή τους.
- Ποινές (Penalties): Το σύστημα διακρίνει δύο είδη παραπτωμάτων:
    1. Inactivity Leak: Εάν ένας κόμβος βγει offline, χάνει σταδιακά μικρό μέρος του κεφαλαίου του. Στόχος είναι να αφαιρεθούν οι ανενεργοί κόμβοι ώστε το δίκτυο να ανακτήσει την οριστικότητα (finality).
    2. Slashing: Είναι η "θανατική ποινή" του PoS. Εάν ένας validator εντοπιστεί να υπογράφει αντικρουόμενα μπλοκ (equivocation), το δίκτυο κατάσχει άμεσα ένα σημαντικό μέρος (π.χ. 32 ETH) ή το σύνολο του κεφαλαίου του και τον αποβάλει βίαια. Αυτό καθιστά την επίθεση εξαιρετικά δαπανηρή [29].

5.3.4 Ειδικά Διανύσματα Επίθεσης στο PoS: Το PoS εισάγει νέες κατηγορίες απειλών που δεν υπήρχαν στο PoW.

Α. Το Πρόβλημα "Nothing at Stake"

Σε περίπτωση διακλάδωσης (fork) στο PoW, ένας miner πρέπει να επιλέξει ποια αλυσίδα θα υποστηρίξει, καθώς δεν έχει αρκετή ενέργεια για να σκάβει και στις δύο. Στο PoS, η "εξόρυξη" δεν κοστίζει τίποτα. Ένας ορθολογικός validator έχει κίνητρο να ψηφίσει και στις δύο αλυσίδες, ώστε να κερδίσει ανεξάρτητα από το ποια θα επικρατήσει. Αυτό εμποδίζει την επίτευξη συναίνεσης.

Λύση: Ο κανόνας του Slashing. Αν ψηφίσεις και στις δύο, χάνεις τα πάντα.

Β. Επιθέσεις Μεγάλης Εμβέλειας (Long Range Attacks)

Επειδή η δημιουργία μπλοκ στο PoS είναι δωρεάν, ένας επιτιθέμενος θα μπορούσε να αγοράσει παλιά ιδιωτικά κλειδιά (από validators που πούλησαν τα νομίσματά τους πριν χρόνια) και να ξαναγράψει ολόκληρη την ιστορία του Blockchain από το σημείο μηδέν (Genesis block), δημιουργώντας μια εναλλακτική, μακρύτερη αλυσίδα.

Λύση: Η εισαγωγή της Ασθενούς Υποκειμενικότητας (Weak Subjectivity). Οι νέοι κόμβοι που συνδέονται στο δίκτυο δεν εμπιστεύονται τυφλά τη μακρύτερη αλυσίδα (όπως στο Bitcoin), αλλά χρησιμοποιούν πρόσφατα "Σημεία Ελέγχου" (Checkpoints) που θεωρούνται αμετάβλητα. Έτσι, οποιαδήποτε προσπάθεια αναγραφής της ιστορίας πέρα από το checkpoint απορρίπτεται αυτόματα.

5.3.5 Συγκεντρωτισμός Πλούτου (Rich-get-Richer): Μια βασική κριτική των Platt et al. (2021) είναι ότι το PoS τείνει να δημιουργεί ολιγοπώλια. Καθώς οι ανταμοιβές είναι ποσοστιαίες, οι μεγάλοι κάτοχοι συσσωρεύουν πλούτο ταχύτερα από τους μικρούς, αυξάνοντας σταδιακά τον

έλεγχό τους στο δίκτυο. Για την αντιμετώπιση αυτού, πολλά δίκτυα εφαρμόζουν μηχανισμούς "κορεσμού" (saturation), όπου η απόδοση ενός κόμβου μειώνεται αν συγκεντρώσει υπερβολικά μεγάλο μερίδιο κεφαλαίου [29].

5.4 Εναλλακτικά Πρωτόκολλα και Υβριδικά Μοντέλα Συναίνεσης

Ενώ το PoW και το PoS κυριαρχούν, η βιομηχανία έχει αναπτύξει εξειδικευμένους μηχανισμούς για την κάλυψη ειδικών αναγκών, όπως η υψηλή συχνότητα συναλλαγών (HFT) και η εταιρική διακυβέρνηση.

5.4.1 Delegated Proof of Stake (DPoS): Η Αντιπροσωπευτική Δημοκρατία

Το DPoS, που εισήχθη από τον Dan Larimer (BitShares, EOS, Tron), αποτελεί μια μετεξέλιξη του PoS που θυσιάζει μερικώς την αποκέντρωση για χάρη της ταχύτητας.

- Λειτουργία Ψηφοφορίας: Αντί κάθε χρήστης να επικυρώνει συναλλαγές, οι κάτοχοι νομισμάτων "ψηφίζουν" σε πραγματικό χρόνο για να εκλέξουν έναν περιορισμένο αριθμό Υπερ-Αντιπροσώπων (Super Representatives) ή "Μαρτύρων" (Witnesses). Συνήθως, ο αριθμός αυτός είναι μικρός και σταθερός (π.χ. 21 στο EOS, 27 στο Tron).
- Παραγωγή Μπλοκ: Οι εκλεγμένοι αντιπρόσωποι αναλαμβάνουν εκ περιτροπής (round-robin) να παράγουν μπλοκ. Επειδή οι κόμβοι είναι λίγοι και γνωστοί, δεν χρειάζεται να περιμένουν τη διάδοση του μηνύματος σε όλο τον πλανήτη. Αυτό επιτρέπει χρόνους μπλοκ της τάξης των 0.5 δευτερολέπτων και χιλιάδες TPS.
- Κριτική: Σύμφωνα με τους Lashkari & Musilek (2021), το DPoS είναι επιρρεπές στη δημιουργία "καρτέλ". Οι αντιπρόσωποι μπορούν να συνεννοηθούν μεταξύ τους για να διατηρήσουν την εξουσία, ενώ η απάθεια των ψηφοφόρων (voter apathy) συχνά οδηγεί σε συγκέντρωση ισχύος σε μεγάλα ανταλλακτήρια που ψηφίζουν με τα νομίσματα των πελατών τους [18].

5.4.2 Proof of History (PoH): Ο Χρόνος ως Κρυπτογραφική Απόδειξη

Το PoH δεν είναι αυτόνομος αλγόριθμος συναίνεσης, αλλά ένας μηχανισμός χρονισμού που λειτουργεί συνδυαστικά με το PoS στο δίκτυο Solana. Επιλύει το πρόβλημα του συγχρονισμού του χρόνου στα κατανεμημένα συστήματα.

- Verifiable Delay Functions (VDFs): Το PoH χρησιμοποιεί μια αναδρομική συνάρτηση hash (SHA-256), όπου η είσοδος της επόμενης επανάληψης είναι η έξοδος της προηγούμενης: $Hash_n$= SHA256($Hash_{n-1}$).
- Η Λογική: Αυτή η διαδικασία είναι αυστηρά σειριακή και δεν μπορεί να παραλληλιστεί. Επομένως, η παραγωγή της ακολουθίας απαιτεί *πραγματικό χρόνο*. Όταν ένας κόμβος παρουσιάζει μια έξοδο hash, αποδεικνύει κρυπτογραφικά ότι έχει περάσει συγκεκριμένος χρόνος.
- Αποτέλεσμα: Οι κόμβοι δεν χρειάζεται να επικοινωνούν μεταξύ τους για να συμφωνήσουν "τι ώρα είναι". Μπορούν να επεξεργάζονται συναλλαγές ασύγχρονα, επιτυγχάνοντας θεωρητικές ταχύτητες έως 65.000 TPS, πλησιάζοντας τις επιδόσεις της Visa [34].

5.4.3 Proof of Authority (PoA): Η Ταυτότητα ως Εγγύηση: Το PoA χρησιμοποιείται κυρίως σε ιδιωτικά (Private) και κοινοπρακτικά (Consortium) δίκτυα, όπως το VeChain και το Microsoft Azure Blockchain.

- Λειτουργία: Το δικαίωμα παραγωγής μπλοκ δεν βασίζεται σε υπολογιστική ισχύ ή πλούτο, αλλά στην Ταυτότητα. Οι επικυρωτές είναι γνωστές οντότητες (π.χ. Τράπεζες, Ελεγκτικές Εταιρείες) που έχουν περάσει από αυστηρό έλεγχο KYC.
- Κίνητρο: Οι επικυρωτές διακυβεύουν τη φήμη τους (Reputation). Εάν ένας επικυρωτής δράσει κακόβουλα, η ταυτότητά του είναι γνωστή και θα υποστεί νομικές και κοινωνικές συνέπειες εκτός δικτύου.
- Πλεονεκτήματα: Εξαλείφει την ανάγκη για σπατάλη ενέργειας και επιτρέπει εξαιρετικά υψηλή απόδοση, καθώς ο αριθμός των κόμβων είναι μικρός και η εμπιστοσύνη δεδομένη.

5.4.4 Federated Byzantine Agreement (FBA): Το Μοντέλο της Εμπιστοσύνης

Σε αντίθεση με τα παραδοσιακά BFT συστήματα που απαιτούν καθολική συμφωνία (όλοι μιλούν με όλους), το FBA (που χρησιμοποιείται από το Stellar και το Ripple/XRP) εισάγει την έννοια των "Φετών Απαρτίας" (Quorum Slices).

- Λειτουργία: Κάθε κόμβος δεν εμπιστεύεται όλο το δίκτυο, αλλά επιλέγει μια λίστα εμπίστων κόμβων (τη "φέτα" του). Για να επικυρωθεί μια συναλλαγή, αρκεί να συμφωνήσουν οι κόμβοι της φέτας του.
- Αναδυόμενη Συναίνεση: Επειδή οι φέτες των κόμβων αλληλο-επικαλύπτονται (ο κόμβος Α εμπιστεύεται τον Β, ο Β τον Γ), η συμφωνία διαδίδεται αλυσιδωτά σε όλο το δίκτυο χωρίς να χρειάζεται κεντρικός συντονισμός.
- Ασφάλεια: Σύμφωνα με τους Mazzeo et al. (2020), το μοντέλο αυτό είναι εξαιρετικά ανθεκτικό σε επιθέσεις Sybil, καθώς ένας επιτιθέμενος πρέπει να πείσει τους τίμιους κόμβους να τον συμπεριλάβουν στις λίστες εμπιστοσύνης τους, κάτι που είναι κοινωνικά δύσκολο [35].

5.4.5 Συγκριτική Αξιολόγηση Αλγορίθμων: Η επιλογή του αλγορίθμου καθορίζει τη φύση του Blockchain.

- DPoS: Ιδανικό για εφαρμογές Gaming και Social Media όπου η ταχύτητα είναι κρίσιμη και η μερική κεντρικοποίηση αποδεκτή.
- PoH: Κατάλληλο για αποκεντρωμένα χρηματιστήρια (DEXs) υψηλής συχνότητας που απαιτούν ακριβή χρονοσήμανση εντολών.
- PoA: Η μόνη βιώσιμη λύση για εταιρικά δίκτυα εφοδιαστικής αλυσίδας (Supply Chain) και τραπεζικές κοινοπραξίες.
- FBA: Βέλτιστο για διασυνοριακές πληρωμές (Remittances) λόγω του χαμηλού κόστους και της γρήγορης οριστικότητας (3-5 δευτερόλεπτα).

ΠΙΝΑΚΑΣ 2: Σύγκριση PoW, PoS και DPoS

Χαρακτηριστικό	Proof of Work (PoW)	Proof of Stake (PoS)	Delegated PoS (DPoS)
Πόρος Εξασφάλισης	Υπολογιστική Ισχύς / Ενέργεια	Δεσμευμένο Κεφάλαιο (Stake)	Ψήφοι Αντιπροσώπων (Delegates)
Ενεργειακό Κόστος	Εξαιρετικά Υψηλό	Πολύ Χαμηλό	Πολύ Χαμηλό
Ταχύτητα / TPS	Χαμηλή (~7-15 TPS)	Μεσαία προς Υψηλή	Πολύ Υψηλή (>3.000 TPS)
Βαθμός Αποκέντρωσης	Πολύ Υψηλός	Υψηλός	Χαμηλός / Τάσεις Ολιγοπωλίου
Κύριος Κίνδυνος	Επίθεση 51% (Εξαιρετικά Ακριβή)	Long-Range Attack / "Rich-get-Richer"	Καρτέλ Αντιπροσώπων / Δωροδοκία

5.5 Περιβαλλοντικές Επιπτώσεις, ESG και Βιωσιμότητα

Η ακαδημαϊκή και δημόσια συζήτηση γύρω από το Blockchain τα τελευταία χρόνια κυριαρχείται από το ζήτημα του περιβαλλοντικού αποτυπώματος. Καθώς η κλιματική κρίση καθίσταται η κυρίαρχη παγκόσμια πρόκληση, οι μηχανισμοί συναίνεσης αξιολογούνται πλέον όχι μόνο με βάση την ασφάλεια, αλλά και τη βιωσιμότητά τους.

5.5.1 Κατανάλωση Ενέργειας και Ηλεκτρονικά Απόβλητα (E-Waste): Το ενεργειακό κόστος του Proof of Work είναι εγγενές χαρακτηριστικό του σχεδιασμού του, γνωστό ως "Θερμοδυναμική Ασφάλεια". Για να είναι ασφαλές το δίκτυο, η επίθεση πρέπει να είναι απαγορευτικά ακριβή σε όρους ενέργειας. Ωστόσο, αυτό οδηγεί σε παράπλευρες απώλειες. Εκτός από την κατανάλωση ηλεκτρισμού, το PoW παράγει τεράστιες ποσότητες ηλεκτρονικών αποβλήτων. Οι εξειδικευμένες μηχανές εξόρυξης (ASICs) έχουν μικρό κύκλο ζωής (περίπου 1.5 έτος) και δεν μπορούν να επαναχρησιμοποιηθούν για άλλους σκοπούς (π.χ. gaming ή AI training), όπως οι κάρτες γραφικών. Σύμφωνα με τους Gallersdörfer et al. (2020), τα ετήσια ηλεκτρονικά απόβλητα του δικτύου Bitcoin είναι συγκρίσιμα με αυτά μεσαίου μεγέθους χωρών, δημιουργώντας ένα σημαντικό πρόβλημα διαχείρισης τοξικών υλικών [31].

5.5.2 Ο Ρόλος των Κριτηρίων ESG και η Πράσινη Μετάβαση: Η αυξανόμενη επιρροή των κριτηρίων ESG (Environmental, Social, and Governance) στις επενδυτικές στρατηγικές έχει λειτουργήσει ως καταλύτης για την αλλαγή του τοπίου της εξόρυξης. Θεσμικοί επενδυτές (όπως η BlackRock ή η Tesla) διστάζουν να τοποθετηθούν σε περιουσιακά στοιχεία με υψηλό αποτύπωμα άνθρακα, πιέζοντας τη βιομηχανία να στραφεί σε καθαρές λύσεις. Οι Sedlmeir et al. (2020) αναλύουν πώς αυτή η πίεση έχει οδηγήσει στη δημιουργία του Bitcoin Mining Council, ενός οργανισμού που στοχεύει στη διαφάνεια της ενεργειακής κατανάλωσης. Οι miners αναζητούν πλέον ενεργητικά την "εγκλωβισμένη ενέργεια" (stranded energy) – δηλαδή πλεόνασμα ενέργειας

που παράγεται από Ανανεώσιμες Πηγές (π.χ. υδροηλεκτρικά φράγματα σε περιόδους βροχοπτώσεων ή αιολικά πάρκα τη νύχτα) και δεν μπορεί να αποθηκευτεί ή να μεταφερθεί στο δίκτυο. Με αυτόν τον τρόπο, το mining λειτουργεί ως "αγοραστής έσχατης ανάγκης" (buyer of last resort), επιδοτώντας ουσιαστικά την ανάπτυξη πράσινων υποδομών και σταθεροποιώντας το ηλεκτρικό δίκτυο (grid balancing) [30].

5.5.3 Συγκριτική Αξιολόγηση PoW vs PoS: Η μετάβαση του Ethereum από PoW σε PoS (γνωστή ως "The Merge" το 2022) αποτέλεσε το μεγαλύτερο πείραμα μείωσης αποτυπώματος στην ιστορία της πληροφορικής. Η αλλαγή αυτή μείωσε την παγκόσμια κατανάλωση ενέργειας του δικτύου κατά ~99.95%. Αυτό αποδεικνύει ότι η τεχνολογία Blockchain μπορεί να αποσυνδεθεί από την περιβαλλοντική επιβάρυνση. Ωστόσο, οι υποστηρικτές του Bitcoin αντιτείνουν ότι το PoW είναι απαραίτητο για τη δημιουργία ενός νομίσματος που έχει "κόστος παραγωγής" (όπως ο χρυσός), σε αντίθεση με το PoS που μοιάζει περισσότερο με μετοχικό κεφάλαιο (fiat currency system).

ΚΕΦΑΛΑΙΟ 6: ΕΞΥΠΝΑ ΣΥΜΒΟΛΑΙΑ ΚΑΙ ΑΠΟΚΕΝΤΡΩΜΕΝΕΣ ΕΦΑΡΜΟΓΕΣ

6.1 Εισαγωγή: Από τη Θεωρία στην Πράξη - "Ο Κώδικας ως Νόμος"

Η εμφάνιση των Έξυπνων Συμβολαίων (Smart Contracts) σηματοδότησε τη μετάβαση από το "Διαδίκτυο της Πληροφορίας" (Web 2.0) στο "Διαδίκτυο της Αξίας" (Web 3.0). Ενώ το Bitcoin απέδειξε ότι μπορούμε να μεταφέρουμε χρήματα χωρίς τράπεζες, τα Έξυπνα Συμβόλαια αποδεικνύουν ότι μπορούμε να εκτελέσουμε πολύπλοκες συμφωνίες χωρίς δικηγόρους ή συμβολαιογράφους.

6.1.1 Ιστορική Προέλευση και η Αναλογία του Αυτόματου Πωλητή: Η ιδέα προτάθηκε για πρώτη φορά το 1994 από τον κρυπτογράφο και νομικό Nick Szabo, πολύ πριν την εφεύρεση του Blockchain. Ο Szabo χρησιμοποίησε την αναλογία του Αυτόματου Πωλητή (Vending Machine) για να περιγράψει τη λειτουργία τους:

- Σε μια συμβατική συναλλαγή, υπάρχει ένας πωλητής (άνθρωπος) που μπορεί να κάνει λάθος στα ρέστα ή να αρνηθεί την εξυπηρέτηση.
- Στον αυτόματο πωλητή, η λογική είναι ενσωματωμένη στο υλικό: *"Αν εισαχθούν 2€ + πατηθεί το κουμπί Α1 = δώσε αναψυκτικό + δώσε ρέστα"*. Η διαδικασία είναι αμετάβλητη, αυτόματη και δεν απαιτεί εμπιστοσύνη προς το μηχάνημα, παρά μόνο προς τον μηχανισμό του. Σύμφωνα με τους Wang et al. (2021), το Ethereum υλοποίησε αυτή τη θεωρία σε παγκόσμια κλίμακα, αντικαθιστώντας το φυσικό μηχάνημα με ένα αποκεντρωμένο δίκτυο κόμβων [28].

6.1.2 Τεχνικός Ορισμός και Χαρακτηριστικά: Ένα Έξυπνο Συμβόλαιο δεν είναι "έξυπνο" (δεν έχει τεχνητή νοημοσύνη) και δεν είναι "συμβόλαιο" με τη νομική έννοια. Είναι ένα αυτόνομο πρόγραμμα (script) που ζει στο Blockchain. Σύμφωνα με τους Zarir et al. (2021), διακρίνεται από τέσσερα βασικά χαρακτηριστικά:

1. Αυτονομία (Autonomy): Μόλις το συμβόλαιο ανεβεί (deploy) στο δίκτυο, δεν ελέγχεται πλέον από τον δημιουργό του. Κανείς δεν μπορεί να το "κλείσει" ή να το σταματήσει, εκτός αν έχει προγραμματιστεί εξαρχής να τερματίζεται.
2. Αμετάβλητο (Immutability): Ο κώδικας δεν μπορεί να τροποποιηθεί. Αν ανακαλυφθεί ένα λάθος (bug) μετά την εκκίνηση, δεν υπάρχει τρόπος να διορθωθεί (patching). Πρέπει να δημιουργηθεί νέο συμβόλαιο και να μεταφερθούν όλοι οι χρήστες εκεί.
3. Ντετερμινισμός (Determinism): Το ίδιο input παράγει πάντα το ίδιο output, ανεξάρτητα από το ποιος εκτελεί τον κώδικα ή πότε.
4. Παρατηρησιμότητα (Observability): Ο κώδικας και η κατάσταση (state) του συμβολαίου είναι δημόσια και ορατά σε όλους. Οποιοσδήποτε μπορεί να ελέγξει τη λογική του πριν αλληλεπιδράσει μαζί του [29].

6.1.3 Ο Κύκλος Ζωής ενός Συμβολαίου: Η δημιουργία και εκτέλεση ενός συμβολαίου ακολουθεί μια αυστηρή διαδικασία:

1. Ανάπτυξη (Development): Ο προγραμματιστής γράφει τον κώδικα σε γλώσσα υψηλού επιπέδου (π.χ. Solidity, Vyper).
2. Μεταγλώττιση (Compilation): Ο κώδικας μετατρέπεται σε Bytecode (για να τον διαβάζει η μηχανή) και παράγεται το ABI (Application Binary Interface), που λειτουργεί ως "χάρτης" των συναρτήσεων.
3. Ανάπτυξη στο Δίκτυο (Deployment): Ο δημιουργός στέλνει μια ειδική συναλλαγή στο δίκτυο που περιέχει το Bytecode. Πληρώνει το αντίστοιχο τέλος (Gas fee) και το δίκτυο δεσμεύει μια νέα, μοναδική διεύθυνση για το συμβόλαιο (π.χ. 0x7a25...).
4. Αλληλεπίδραση (Interaction): Οι χρήστες ή άλλα συμβόλαια στέλνουν μηνύματα (transactions) στη διεύθυνση του συμβολαίου για να ενεργοποιήσουν τις συναρτήσεις του.

6.1.4 Συνθεσιμότητα (Composability): Τα "Money Legos" Μια μοναδική ιδιότητα των έξυπνων συμβολαίων, που τονίζεται από τους Werner et al. (2021), είναι η Συνθεσιμότητα. Επειδή όλα τα συμβόλαια ζουν στο ίδιο ανοιχτό δίκτυο (π.χ. Ethereum), μπορούν να αλληλεπιδρούν μεταξύ τους χωρίς να χρειάζεται ειδική άδεια (permissionless integration). Ένα συμβόλαιο δανεισμού μπορεί να καλέσει ένα συμβόλαιο ανταλλακτηρίου, το οποίο με τη σειρά του καλεί ένα συμβόλαιο ασφάλισης. Αυτή η δυνατότητα να χτίζει ο ένας πάνω στον κώδικα του άλλου ονομάζεται συχνά "Money Legos" και αποτελεί τη βάση της εκρηκτικής ανάπτυξης του DeFi. Ένας προγραμματιστής μπορεί να δημιουργήσει μια πολύπλοκη τραπεζική εφαρμογή σε λίγες μέρες, συνδυάζοντας υπάρχοντα, ελεγμένα συμβόλαια [30].

6.1.5 Νομικές Προκλήσεις και Ricardian Contracts: Η φράση *"Code is Law"* υποδηλώνει ότι ο κώδικας είναι η τελική αρχή. Ωστόσο, αυτό δημιουργεί συγκρούσεις με το παραδοσιακό δίκαιο. Εάν ένας χάκερ βρει ένα "παραθυράκι" στον κώδικα και αδειάσει ένα ταμείο,

σύμφωνα με τη λογική του Blockchain, η ενέργεια είναι έγκυρη ("The code allows it"). Σύμφωνα με τον ποινικό κώδικα, είναι κλοπή. Για τη γεφύρωση αυτού του χάσματος, αναπτύσσονται τα Ricardian Contracts: συμβόλαια που είναι αναγνώσιμα τόσο από ανθρώπους (νομικό κείμενο) όσο και από μηχανές (κώδικας), συνδέοντας τη νομική ευθύνη με την ψηφιακή εκτέλεση.

6.2 Η Εικονική Μηχανή του Ethereum (Ethereum Virtual Machine - EVM)

Η EVM αποτελεί τον πυρήνα της λειτουργίας του Ethereum. Είναι μια παγκόσμια, αποκεντρωμένη υπολογιστική μηχανή που διατηρεί την κατάσταση (state) του δικτύου. Κάθε κόμβος του Ethereum τρέχει μια instance της EVM και εκτελεί τις ίδιες εντολές για να επιβεβαιώσει το αποτέλεσμα κάθε συναλλαγής.

6.2.1 Αρχιτεκτονική και Μοντέλο Μνήμης: Σε αντίθεση με τους τυπικούς επεξεργαστές (x86/ARM) που βασίζονται σε καταχωρητές (register-based), η EVM είναι μια αρχιτεκτονική στοίβας (stack-based architecture). Αυτό σημαίνει ότι όλες οι πράξεις γίνονται με την εισαγωγή (PUSH) και εξαγωγή (POP) δεδομένων από μια δομή LIFO (Last-In, First-Out). Σύμφωνα με τους Zarir et al. (2021), η EVM διαχειρίζεται τρεις τύπους μνήμης, ο καθένας με διαφορετικό κόστος και διάρκεια ζωής:

1. Στοίβα (Stack): Έχει μέγιστο βάθος 1024 στοιχείων των 256-bit. Είναι η φθηνότερη μορφή μνήμης αλλά και η πιο περιορισμένη. Χρησιμοποιείται για ενδιάμεσους υπολογισμούς.
2. Μνήμη (Memory): Είναι προσωρινή και διαγράφεται μετά το τέλος της εκτέλεσης της συναλλαγής. Είναι γραμμική και επεκτάσιμη, αλλά το κόστος της αυξάνεται τετραγωνικά όσο μεγαλώνει το μέγεθός της.
3. Αποθήκευση (Storage): Είναι η μόνη μόνιμη μνήμη. Τα δεδομένα που γράφονται εδώ (π.χ. τα υπόλοιπα των λογαριασμών) παραμένουν στο Blockchain για πάντα. Γι' αυτό, η εγγραφή στο Storage είναι η πιο ακριβή λειτουργία σε όρους Gas (opcode SSTORE) [29].

6.2.2 Το Πρόβλημα Τερματισμού και ο Μηχανισμός Gas: Η EVM είναι Turing-Complete, που σημαίνει ότι μπορεί να εκτελέσει οποιονδήποτε αλγόριθμο. Ωστόσο, αυτό δημιουργεί τον κίνδυνο του Προβλήματος Τερματισμού (Halting Problem): ένας κακόβουλος χρήστης θα μπορούσε να γράψει ένα συμβόλαιο με έναν άπειρο βρόχο (while(true) {}), το οποίο θα ανάγκαζε όλους τους κόμβους του πλανήτη να κολλήσουν εκτελώντας το για πάντα. Η λύση είναι ο μηχανισμός του Gas. Κάθε εντολή κοστίζει μονάδες ενέργειας.

- EIP-1559 και Δυναμική Τιμολόγηση: Από το 2021 (London Hard Fork), το κόστος χωρίζεται σε Base Fee (που καίγεται/καταστρέφεται) και Priority Fee (που πηγαίνει στον validator). Αν ο χρήστης δεν έχει αρκετό ETH για να πληρώσει το Gas, η EVM σταματά την εκτέλεση και αναιρεί όλες τις αλλαγές (Revert), αλλά κρατά τα τέλη [30].

6.2.3 Κωδικοί Λειτουργίας (Opcodes) και Bytecode: Οι προγραμματιστές γράφουν σε Solidity, αλλά η EVM καταλαβαίνει μόνο Bytecode. Το Bytecode είναι μια σειρά από δεκαεξαδικούς

αριθμούς που αντιστοιχούν σε συγκεκριμένες εντολές (Opcodes). Μερικά χαρακτηριστικά παραδείγματα:

- 0x60 (PUSH1): Βάζει ένα byte στη στοίβα.
- 0x01 (ADD): Προσθέτει τα δύο πρώτα στοιχεία της στοίβας.
- 0x55 (SSTORE): Αποθηκεύει μια τιμή στη μόνιμη μνήμη (το πιο ακριβό opcode).
- 0xA0 (LOG0): Καταγράφει ένα γεγονός (Event) που είναι ορατό εκτός αλυσίδας αλλά όχι από άλλα συμβόλαια. Η κατανόηση των Opcodes είναι κρίσιμη για τη βελτιστοποίηση του κόστους Gas (Gas Optimization).

6.2.4 Μηνύματα και Κλήσεις (Message Calls vs DelegateCalls): Τα συμβόλαια μπορούν να αλληλεπιδρούν μεταξύ τους μέσω "εσωτερικών συναλλαγών". Υπάρχουν δύο τύποι κλήσεων με τεράστια διαφορά ασφαλείας:

1. CALL: Το συμβόλαιο Α καλεί το συμβόλαιο Β. Ο κώδικας του Β εκτελείται στο περιβάλλον του Β (με τα δικά του storage variables).
2. DELEGATECALL: Το συμβόλαιο Α καλεί το συμβόλαιο Β, αλλά ο κώδικας του Β εκτελείται στο περιβάλλον του Α. Όπως εξηγούν οι Werner et al. (2021), το DELEGATECALL είναι το κλειδί για τα Αναβαθμίσιμα Συμβόλαια (Upgradable Contracts). Ένα συμβόλαιο-Proxy κρατάει την κατάσταση (state) και τα χρήματα, ενώ αναθέτει τη λογική σε ένα άλλο συμβόλαιο-Logic. Αν βρεθεί bug, απλώς αλλάζουμε τη διεύθυνση του Logic contract, διατηρώντας τα δεδομένα άθικτα στο Proxy. Ωστόσο, η λανθασμένη χρήση του έχει οδηγήσει σε χακάρισμα εκατομμυρίων (π.χ. Parity Wallet Hack) [30].

6.2.5 Παγκόσμια Κατάσταση και Merkle Patricia Trie: Η "κατάσταση" του Ethereum (ποιος έχει πόσα χρήματα, ποιο είναι το nonce κάθε λογαριασμού) δεν αποθηκεύεται σε έναν απλό πίνακα, αλλά σε μια δομή δεδομένων που ονομάζεται Merkle Patricia Trie. Πρόκειται για έναν συνδυασμό Merkle Tree (για κρυπτογραφική επαλήθευση) και Patricia Trie (για γρήγορη αναζήτηση κλειδιών). Κάθε φορά που αλλάζει έστω και ένα υπόλοιπο λογαριασμού μετά από μια συναλλαγή, αλλάζει η ρίζα του δέντρου (State Root). Αυτή η ρίζα μπαίνει στην επικεφαλίδα του μπλοκ, επιτρέποντας στους Light Clients (π.χ. κινητά τηλέφωνα) να επιβεβαιώσουν την ύπαρξη μιας συναλλαγής χωρίς να κατεβάσουν ολόκληρο το Blockchain [31].

6.3 Πρότυπα Token και Διαλειτουργικότητα (ERC Standards)

Η επιτυχία του Ethereum δεν οφείλεται μόνο στην EVM, αλλά κυρίως στην τυποποίηση. Μέσω των Ethereum Request for Comments (ERC), η κοινότητα συμφώνησε σε κοινά πρωτόκολλα (interfaces). Χωρίς αυτά, κάθε πορτοφόλι (π.χ. MetaMask) θα έπρεπε να γράφει προσαρμοσμένο κώδικα για κάθε νέο token που κυκλοφορεί.

6.3.1 ERC-20: Το Πρότυπο των Εναλλάξιμων Νομισμάτων (Fungible Tokens): Το ERC-20, που προτάθηκε το 2015, είναι το κυρίαρχο πρότυπο για τη δημιουργία νομισμάτων

(tokens). Ορίζει ότι κάθε μονάδα του token είναι πανομοιότυπη με οποιαδήποτε άλλη (Fungibility), ακριβώς όπως ένα ευρώ είναι ίσο με ένα άλλο ευρώ.

Σύμφωνα με τους Chen et al. (2020), η δομή του βασίζεται σε έναν πίνακα αντιστοίχισης (mapping) address => uint256, ο οποίος καταγράφει το υπόλοιπο κάθε χρήστη. Οι βασικές συναρτήσεις που πρέπει να υλοποιεί είναι:

- function totalSupply() public view returns (uint256)
- function balanceOf(address account) public view returns (uint256)
- function transfer(address recipient, uint256 amount) public returns (bool)

Το Ζήτημα Ασφαλείας του approve και transferFrom

Το ERC-20 εισήγαγε έναν μηχανισμό για να επιτρέπει σε τρίτους (π.χ. ανταλλακτήρια DEX) να ξοδεύουν tokens εκ μέρους του χρήστη.

1. Ο χρήστης καλεί την approve(spender, amount).
2. Το συμβόλαιο του DEX καλεί την transferFrom(sender, recipient, amount).

Ωστόσο, όπως επισημαίνουν οι Zhang et al. (2020), αυτό αποτελεί μείζον διάνυσμα επίθεσης. Οι χρήστες συχνά εγκρίνουν "απεριόριστο ποσό" $2^{256} - 1$ για ευκολία. Εάν το συμβόλαιο του DEX παραβιαστεί, ο επιτιθέμενος μπορεί να αδειάσει το πορτοφόλι του χρήστη χωρίς να χρειάζεται το ιδιωτικό του κλειδί, καθώς έχει ήδη την έγκριση (Infinite Approval Risk) [20].

6.3.2 ERC-721: Μη-Εναλλάξιμα Tokens (Non-Fungible Tokens - NFTs): Το ERC-721 έφερε την επανάσταση της ψηφιακής ιδιοκτησίας. Σε αντίθεση με το ERC-20, εδώ κάθε token είναι μοναδικό και διακρίνεται από ένα tokenId.

Η δομή δεδομένων αλλάζει από address => amount σε tokenId => owner.

Βασικά χαρακτηριστικά σύμφωνα με τους Wang et al. (2021):

- Metadata: Κάθε token συνδέεται με ένα URI (Uniform Resource Identifier) που δείχνει σε ένα αρχείο JSON (συνήθως στο IPFS), το οποίο περιέχει την εικόνα, το όνομα και τα χαρακτηριστικά του αντικειμένου.
- SafeTransfer: Το πρότυπο εισήγαγε τη συνάρτηση safeTransferFrom, η οποία ελέγχει αν ο παραλήπτης είναι έξυπνο συμβόλαιο. Αν είναι, ελέγχει αν το συμβόλαιο έχει υλοποιήσει τον κατάλληλο δέκτη (receiver hook). Αν όχι, η συναλλαγή αποτυγχάνει. Αυτό λύνει το πρόβλημα των "χαμένων tokens" που στέλνονταν κατά λάθος σε συμβόλαια που δεν μπορούσαν να τα διαχειριστούν [28].

6.3.3 ERC-1155: Το Υβριδικό Πρότυπο Πολλαπλών Tokens: Αναπτύχθηκε από την εταιρεία Enjin για τις ανάγκες της βιομηχανίας Gaming. Το πρόβλημα με τα προηγούμενα πρότυπα ήταν ότι αν ένα παιχνίδι είχε 100 διαφορετικά αντικείμενα (σπαθιά, ασπίδες, νομίσματα), έπρεπε να αναπτύξει (deploy) 100 ξεχωριστά συμβόλαια ERC-721, αυξάνοντας δραματικά το κόστος Gas.

Το ERC-1155 επιτρέπει τη διαχείριση Fungible, Non-Fungible και Semi-Fungible tokens μέσα από ένα και μοναδικό συμβόλαιο.

- Batch Transfers: Επιτρέπει τη μαζική μεταφορά πολλών διαφορετικών tokens με μία μόνο συναλλαγή (safeBatchTransferFrom), μειώνοντας το κόστος μεταφοράς κατά ~90%.

- Ενιαίο ID Space: Κάθε token έχει ID, αλλά μπορεί να έχει και ποσότητα μεγαλύτερη του 1 (όπως στο ERC-20).

6.3.4 Νεότερα Πρότυπα: Soulbound και Tokenized Vaults: Η εξέλιξη δεν σταμάτησε στο 2018. Η περίοδος 2022-2024 έφερε νέα πρότυπα για εξειδικευμένες χρήσεις.

- SBT (Soulbound Tokens - EIP-5192): Πρόκειται για NFTs που είναι μη-μεταβιβάσιμα (non-transferable). Μόλις ληφθούν από μια διεύθυνση, δεν μπορούν να σταλούν αλλού. Χρησιμοποιούνται για την ψηφιακή ταυτότητα, πτυχία πανεπιστημίου ή πιστοποιητικά KYC, καθώς αντιπροσωπεύουν ιδιότητες που είναι εγγενείς στο άτομο και δεν πωλούνται.
- ERC-4626 (Tokenized Vaults): Τυποποίησε τον τρόπο που λειτουργούν τα "θησαυροφυλάκια" (Vaults) στο DeFi. Πριν το 4626, κάθε πλατφόρμα (Aave, Compound, Yearn) είχε δικό της τρόπο να υπολογίζει τις αποδόσεις (yield). Τώρα, υπάρχει ένα κοινό interface για την κατάθεση (deposit) και ανάληψη (withdraw) περιουσιακών στοιχείων που τοκίζονται, επιτρέποντας την εύκολη διασύνδεση εφαρμογών [36].

6.3.5 Συγκριτική Ανάλυση και Κόστος Gas: Σύμφωνα με μετρήσεις των Zarir et al. (2021), η επιλογή προτύπου επηρεάζει δραματικά το κόστος λειτουργίας.

- Η δημιουργία (minting) ενός ERC-721 κοστίζει περίπου 96.000 gas.
- Η δημιουργία ενός ERC-1155 (ακόμα και για πολλαπλά αντικείμενα) μπορεί να κοστίσει μόλις 50.000 gas λόγω βελτιστοποίησης αποθήκευσης.

Ωστόσο, το ERC-721 παραμένει το πρότυπο για υψηλής αξίας ψηφιακή τέχνη λόγω της απλότητας και της ευρείας υποστήριξής του από πλατφόρμες όπως το OpenSea.

6.4 Αποκεντρωμένη Χρηματοδότηση (DeFi): Πρωτόκολλα και Μηχανισμοί

Η Αποκεντρωμένη Χρηματοδότηση (DeFi) αντιπροσωπεύει τη μετάβαση από τα παραδοσιακά, κεντρικοποιημένα χρηματοπιστωτικά συστήματα (CeFi) σε ένα ανοιχτό, διαφανές και χωρίς άδειες (permissionless) οικοσύστημα. Βασίζεται στη σύνθεση τυποποιημένων έξυπνων συμβολαίων ("Money Legos") για τη δημιουργία πολύπλοκων χρηματοοικονομικών προϊόντων.

Σύμφωνα με την εκτενή επισκόπηση των Werner et al. (2021), το DeFi διαφέρει θεμελιωδώς από το CeFi ως προς τη διαχείριση του κινδύνου: στο CeFi ο κίνδυνος αναλαμβάνεται από τον διαμεσολαβητή (Τράπεζα), ενώ στο DeFi ο κίνδυνος ελέγχεται αλγοριθμικά από τον κώδικα (Smart Contract Risk) [30].

6.4.1 Αποκεντρωμένα Ανταλλακτήρια (DEXs) και AMMs: Τα πρώτα DEXs προσπάθησαν να αντιγράψουν το μοντέλο του "Βιβλίου Εντολών" (Central Limit Order Book - CLOB) των παραδοσιακών χρηματιστηρίων. Ωστόσο, λόγω του κόστους Gas και της

καθυστέρησης των μπλοκ στο Ethereum, αυτό το μοντέλο απέτυχε. Η λύση δόθηκε από τους Automated Market Makers (AMMs), όπως το Uniswap.

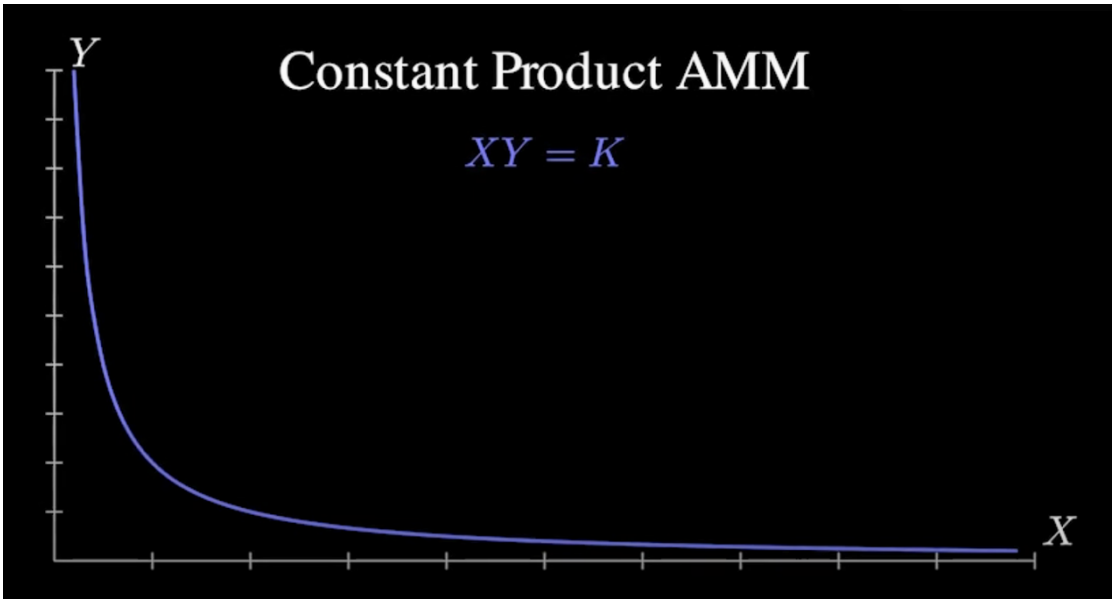
A. Το Μαθηματικό Μοντέλο Constant Product

Ο πυρήνας ενός AMM είναι η εξίσωση του "Σταθερού Γινομένου":

$$x \times y = k$$

Όπου:

- x: Η ποσότητα του νομίσματος Α στη δεξαμενή (π.χ. ETH).
- y: Η ποσότητα του νομίσματος Β στη δεξαμενή (π.χ. USDT).
- k: Μια σταθερά που πρέπει να παραμένει αμετάβλητη κατά τη διάρκεια μιας συναλλαγής.



Εικόνα 6.1: Η καμπύλη του αλγορίθμου Σταθερού Γινομένου ($x \times y = k$) που χρησιμοποιείται στους Αυτοματοποιημένους Ειδικούς Διαπραγματευτές (AMMs).

Όταν ένας χρήστης θέλει να αγοράσει ποσότητα Δx(αφαιρώντας την από τη δεξαμενή), πρέπει να καταθέσει ποσότητα Δy ώστε το γινόμενο να παραμείνει k.

Η νέα τιμή (P') καθορίζεται από την αναλογία των αποθεμάτων μετά τη συναλλαγή. Όσο μεγαλύτερη είναι η παραγγελία σε σχέση με το μέγεθος της δεξαμενής (Liquidity Depth), τόσο μεγαλύτερη είναι η Ολίσθηση Τιμής (Price Slippage).

Β. Μη-Μόνιμη Ζημία (Impermanent Loss - IL)

Οι Πάροχοι Ρευστότητας (Liquidity Providers - LPs) που καταθέτουν τα κεφάλαιά τους σε AMMs αντιμετωπίζουν έναν μοναδικό κίνδυνο. Εάν η εξωτερική τιμή αγοράς ενός νομίσματος αλλάξει δραματικά σε σχέση με την τιμή κατάθεσης, ο αλγόριθμος του AMM θα "πουλήσει" αυτόματα το ανατιμημένο νόμισμα για να αγοράσει το υποτιμημένο (εξισορρόπηση).

Σύμφωνα με τους Loesch et al. (2021), η Μη-Μόνιμη Ζημία είναι η διαφορά στην αξία του χαρτοφυλακίου μεταξύ της απλής διακράτησης (HODL) και της παροχής ρευστότητας. Ονομάζεται "μη-μόνιμη" γιατί αν η τιμή επιστρέψει στην αρχική της ισοτιμία, η ζημία εξαφανίζεται. Αν όμως ο LP αποσύρει τα κεφάλαια ενώ η τιμή είναι διαφορετική, η ζημία πραγματοποιείται [37].

6.4.2 Πρωτόκολλα Δανεισμού και Υπερ-Εξασφάλιση: Πλατφόρμες όπως το Aave και το Compound επιτρέπουν τον δανεισμό χωρίς πιστωτικό έλεγχο (credit check). Πώς διασφαλίζεται ότι ο δανειολήπτης θα πληρώσει; Μέσω της Υπερ-Εξασφάλισης (Over-collateralization).

Για να δανειστεί κάποιος αξία $100 σε USDT, πρέπει να κλειδώσει ως ενέχυρο (collateral) αξία $150 σε ETH.

Α. Συντελεστής Υγείας (Health Factor)

Η ασφάλεια του συστήματος παρακολουθείται μέσω του Health Factor (H_f):

$$H_f = \frac{\sum(Collateral\ Value_i \times Liquidation\ Threshold_i)}{\sum Total\ Borrows_j}$$

- Αν H_f > 1: Το δάνειο είναι ασφαλές.
- Αν H_f < 1: Το δάνειο κινδυνεύει και ενεργοποιείται η διαδικασία ρευστοποίησης.

Β. Μηχανισμός Ρευστότητας (Liquidations)

Εάν η τιμή του ενεχύρου (ETH) πέσει και το H_f πέσει κάτω από το 1, το έξυπνο συμβόλαιο επιτρέπει σε τρίτους ("Liquidators") να αποπληρώσουν μέρος του δανείου εκ μέρους του δανειολήπτη. Ως ανταμοιβή, λαμβάνουν το ισοδύναμο ποσό του ενεχύρου συν ένα μπόνους (Liquidation Bonus, π.χ. 5-10%). Αυτό δημιουργεί ένα ανταγωνιστικό οικοσύστημα από bots που παρακολουθούν το δίκτυο για επισφαλή δάνεια [38].

6.4.3 Flash Loans: Αρμπιτράζ Χωρίς Κεφάλαιο: Τα Flash Loans, που εισήχθησαν από την πλατφόρμα Aave, αποτελούν μια καινοτομία που δεν έχει αντίστοιχο στον παραδοσιακό χρηματοπιστωτικό τομέα. Επιτρέπουν τον δανεισμό απεριόριστου κεφαλαίου χωρίς καμία εγγύηση, υπό μία αυστηρή προϋπόθεση: το δάνειο πρέπει να ληφθεί και να αποπληρωθεί μέσα στην ίδια συναλλαγή (Atomic Transaction).

Α. Η Λογική της Ατομικότητας

Στο Ethereum, μια συναλλαγή μπορεί να περιλαμβάνει πολλές εντολές. Εάν οποιαδήποτε εντολή αποτύχει, ολόκληρη η συναλλαγή αναιρείται (revert).

Ένας χρήστης μπορεί να γράψει ένα συμβόλαιο που:

1. Δανείζεται 10.000.000 USDC από το Aave.
2. Αγοράζει ETH στο Uniswap (όπου η τιμή είναι χαμηλή).
3. Πουλάει το ETH στο SushiSwap (όπου η τιμή είναι υψηλή).
4. Επιστρέφει τα 10.000.000 USDC στο Aave + 0.09% τέλος.
5. Κρατάει το κέρδος.

Εάν στο βήμα (3) το κέρδος δεν επαρκεί για να καλύψει το δάνειο, η εντολή (4) αποτυγχάνει, και η EVM ακυρώνει όλη τη διαδικασία. Ο χρήστης χάνει μόνο το κόστος του Gas.

Β. Κίνδυνοι και Επιθέσεις (Flash Loan Attacks)

Σύμφωνα με τους Qin et al. (2021), τα Flash Loans χρησιμοποιούνται συχνά για επιθέσεις χειραγώγησης τιμών. Ένας επιτιθέμενος μπορεί να δανειστεί τεράστια ρευστότητα για να αλλοιώσει προσωρινά την τιμή σε ένα DEX, ξεγελώντας ένα άλλο πρωτόκολλο που βασίζεται σε αυτή την τιμή (Oracle Manipulation), και να αποκομίσει παράνομα κέρδη [32].

6.4.4 Yield Farming και Governance Tokens: Το καλοκαίρι του 2020 ("DeFi Summer") χαρακτηρίστηκε από την εμφάνιση του Yield Farming. Τα πρωτόκολλα, για να προσελκύσουν ρευστότητα, άρχισαν να επιβραβεύουν τους χρήστες όχι μόνο με τόκους, αλλά και με Governance

Tokens (π.χ. COMP, UNI). Αυτά τα tokens δίνουν δικαίωμα ψήφου για τη διαχείριση του πρωτοκόλλου (DAO), μετατρέποντας τους χρήστες σε μετόχους.

Οι Aggregators (όπως το Yearn Finance) αυτοματοποιούν αυτή τη διαδικασία. Το έξυπνο συμβόλαιο μετακινεί τα κεφάλαια των χρηστών μεταξύ διαφορετικών πρωτοκόλλων (Lending, Liquidity Pools) αναζητώντας συνεχώς την υψηλότερη απόδοση (APY), λειτουργώντας ως ένας "αυτόματος διαχειριστής κεφαλαίων".

6.5 Το Πρόβλημα των Χρησμών (The Oracle Problem)

Τα blockchains όπως το Ethereum είναι σχεδιασμένα ως κλειστά, ντετερμινιστικά συστήματα. Έχουν πλήρη γνώση για το τι συμβαίνει "μέσα" στο δίκτυο (συναλλαγές, υπόλοιπα), αλλά έχουν πλήρη άγνοια για τον έξω κόσμο. Αυτός ο περιορισμός δεν είναι σφάλμα σχεδιασμού, αλλά χαρακτηριστικό ασφαλείας.

Το Πρόβλημα των Χρησμών ορίζεται ως η αδυναμία των έξυπνων συμβολαίων να έχουν πρόσβαση σε εξωτερικά δεδομένα (off-chain data) χωρίς να διακυβεύεται η αξιοπιστία της συναίνεσης.

6.5.1 Η Ανάγκη για Ντετερμινισμό: Γιατί το Ethereum δεν μπορεί απλώς να κάνει ένα API Call στο Google για να μάθει την τιμή του Bitcoin;

Σύμφωνα με τους Beniiche (2020), αν επιτρεπόταν η πρόσβαση στο διαδίκτυο, κάθε κόμβος που θα εκτελούσε το συμβόλαιο θα έπαιρνε διαφορετική απάντηση, ανάλογα με:

- Τον χρόνο εκτέλεσης (η τιμή αλλάζει κάθε δευτερόλεπτο).
- Τη γεωγραφική τοποθεσία (διαφορετικά CDN servers).
- Τη διαθεσιμότητα της ιστοσελίδας (404 Error).

Αυτό θα οδηγούσε σε αποτυχία συναίνεσης, καθώς οι κόμβοι δεν θα συμφωνούσαν ποτέ στο τελικό αποτέλεσμα (State Root). Γι' αυτό, τα δεδομένα πρέπει να εισαχθούν στο Blockchain *πριν* χρησιμοποιηθούν, μέσω μιας ειδικής συναλλαγής [31].

6.5.2 Ταξινομία και Κατηγορίες Χρησμών: Η βιβλιογραφία διακρίνει τους Χρησμούς σε κατηγορίες ανάλογα με την πηγή και την κατεύθυνση της πληροφορίας.

- Λογισμικού (Software Oracles): Αντλούν δεδομένα από online πηγές (APIs, ιστοσελίδες). Είναι οι πιο συνηθισμένοι στο DeFi (τιμές νομισμάτων).
- Υλικού (Hardware Oracles): Αντλούν δεδομένα από τον φυσικό κόσμο μέσω αισθητήρων IoT. Παράδειγμα: Ένα έξυπνο συμβόλαιο ασφάλισης αγροτικής παραγωγής που πληρώνει αυτόματα αν ένας αισθητήρας μετρήσει ξηρασία για 30 μέρες.
- Εισερχόμενοι (Inbound): Φέρνουν δεδομένα *στο* Blockchain (π.χ. "Ποιος κέρδισε τις εκλογές;").
- Εξερχόμενοι (Outbound): Στέλνουν εντολές *στον* έξω κόσμο (π.χ. "Ξεκλείδωσε την έξυπνη κλειδαριά Airbnb μόλις πληρωθεί το ενοίκιο").

- Συναίνεσης (Consensus-based): Χρησιμοποιούν την πρόβλεψη αγορών (Prediction Markets, όπως το Augur) για να καθορίσουν την αλήθεια μέσω της σοφίας του πλήθους.

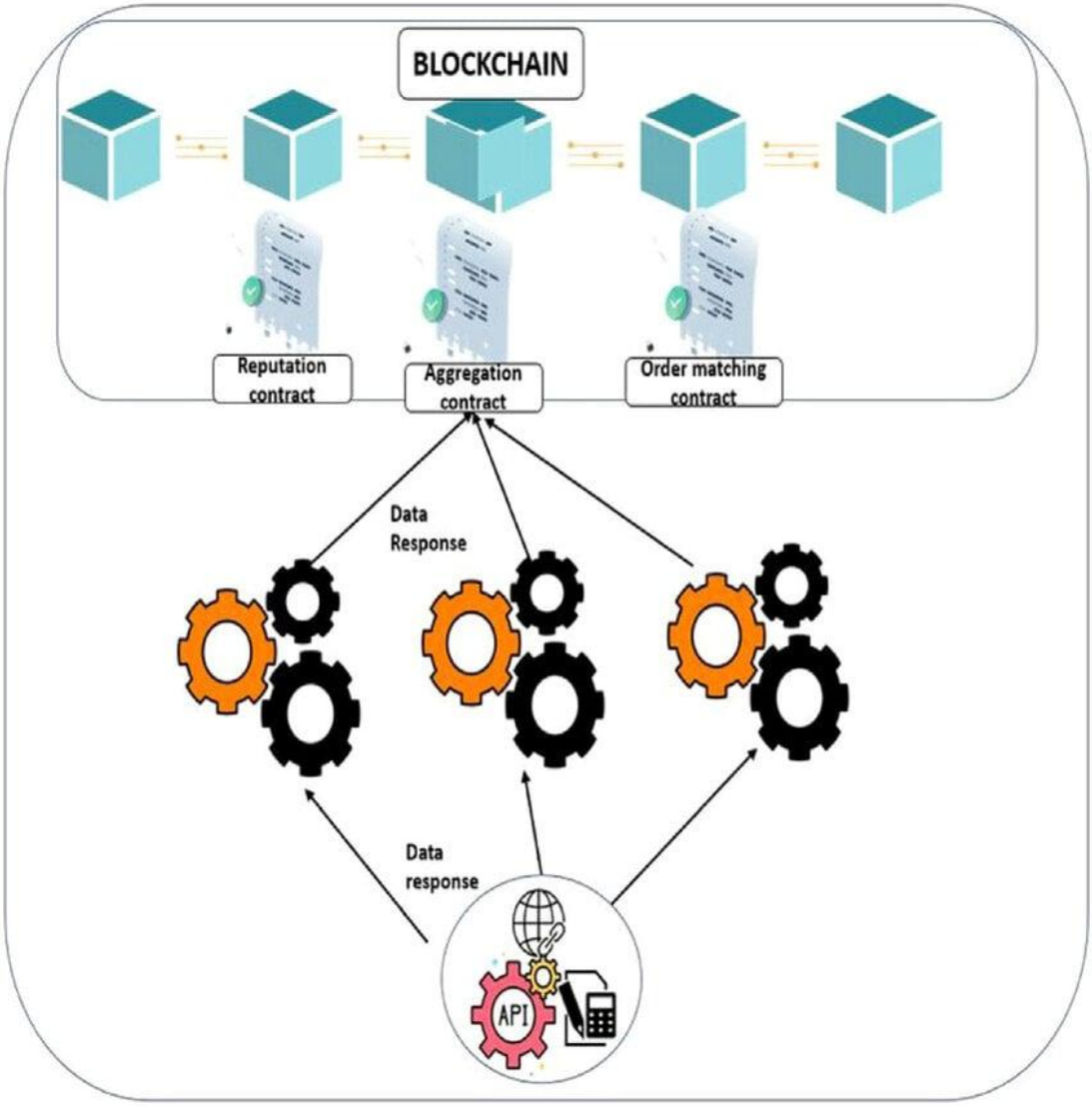
6.5.3 Αποκεντρωμένα Δίκτυα Χρησμών (DONs) και Chainlink: Ένας

κεντρικοποιημένος Χρησμός (π.χ. ένας server της Coinbase που ανεβάζει τιμές) αποτελεί "Μοναδικό Σημείο Αποτυχίας" (Single Point of Failure). Αν χακαριστεί ή δωροδοκηθεί, ολόκληρο το DeFi οικοσύστημα καταρρέει.

Η λύση είναι τα Decentralized Oracle Networks (DONs), με κυρίαρχο το Chainlink.

Σύμφωνα με τους Breidenbach et al. (2021), η αρχιτεκτονική λειτουργεί ως εξής:

1. Request: Το έξυπνο συμβόλαιο ζητά την τιμή του ETH/USD.
2. Aggregation: Το δίκτυο Chainlink επιλέγει τυχαία 20-30 κόμβους (Oracles).
3. Data Fetching: Κάθε κόμβος παίρνει την τιμή από διαφορετική πηγή (Binance, Kraken, CoinGecko).
4. Consensus: Οι κόμβοι υποβάλλουν τις τιμές τους. Το πρωτόκολλο απορρίπτει τις ακραίες τιμές (outliers) και υπολογίζει τη διάμεσο (median).
5. Response: Η τελική, aggregated τιμή γράφεται στο Blockchain και είναι αυτή που χρησιμοποιεί το συμβόλαιο [39].



Εικόνα 6.2: Αρχιτεκτονική ενός Αποκεντρωμένου Δικτύου Χρησμών (DON) για την ασφαλή και αξιόπιστη εισαγωγή εξωτερικών δεδομένων στο Blockchain.

6.5.4 Επιθέσεις Χειραγώγησης και TWAP: Μια από τις πιο επικίνδυνες επιθέσεις στο DeFi είναι η Χειραγώγηση του Χρησμού (Oracle Manipulation). Συμβαίνει όταν ένα πρωτόκολλο βασίζεται σε *μία μόνο* πηγή για την τιμή, συνήθως ένα DEX (π.χ. Uniswap Spot Price).

- Το σενάριο επίθεσης: Ένας επιτιθέμενος χρησιμοποιεί ένα Flash Loan για να αγοράσει μαζικά ένα token στο Uniswap, εκτοξεύοντας τεχνητά την τιμή του. Την ίδια στιγμή, καταθέτει αυτό το token ως ενέχυρο σε μια πλατφόρμα δανεισμού που διαβάζει την τιμή από το Uniswap. Το σύστημα "ξεγελιέται", νομίζει ότι το ενέχυρο αξίζει εκατομμύρια και επιτρέπει στον επιτιθέμενο να δανειστεί (και να κλέψει) όλα τα διαθέσιμα κεφάλαια.
- Η Λύση TWAP (Time-Weighted Average Price): Για να αντιμετωπιστεί αυτό, χρησιμοποιείται ο Μέσος Σταθμικός Όρος Χρόνου. Αντί να πάρουμε την τρέχουσα τιμή (που μπορεί να χειραγωγηθεί στιγμιαία), παίρνουμε τον μέσο όρο της τιμής για τα τελευταία n μπλοκ.

Ο τύπος υπολογισμού είναι:

$$P_{TWAP} = \frac{\sum_{i=1}^{n} P_i \times T_i}{\sum_{i=1}^{n} T_i}$$

Όπου P_i η τιμή και T_i η χρονική διάρκεια.

Σύμφωνα με τους Caldarelli (2020), το TWAP καθιστά την επίθεση εξαιρετικά δαπανηρή, καθώς ο επιτιθέμενος θα έπρεπε να κρατήσει την τιμή τεχνητά ψηλά για μεγάλο χρονικό διάστημα, κάτι που απαιτεί τεράστια κεφάλαια και εγκυμονεί κίνδυνο arbitrage από τρίτους [40].

6.6 Αποκεντρωμένες Εφαρμογές (DApps) και Οικοσύστημα DeFi

Ενώ τα Έξυπνα Συμβόλαια είναι ο κώδικας που τρέχει στο παρασκήνιο (backend), οι Αποκεντρωμένες Εφαρμογές (DApps) είναι η διεπαφή που επιτρέπει στον χρήστη να αλληλεπιδράσει με αυτόν τον κώδικα. Η έκρηξη καινοτομίας που προκλήθηκε από τις DApps οδήγησε στη δημιουργία της Αποκεντρωμένης Χρηματοοικονομικής (DeFi), ενός παράλληλου τραπεζικού συστήματος που λειτουργεί χωρίς κεντρικούς διαμεσολαβητές.

6.6.1 Αρχιτεκτονική ενός DApp: Web 2.0 vs Web 3.0: Η θεμελιώδης διαφορά ενός DApp από μια συμβατική εφαρμογή (π.χ. Facebook) εντοπίζεται στη διαχείριση των δεδομένων και της λογικής. Σύμφωνα με τους Wu et al. (2021), η αρχιτεκτονική Web 3.0 αποτελείται από τρία επίπεδα:

1. Front-end: Η ιστοσελίδα (HTML/JS) που βλέπει ο χρήστης. Μοιάζει με τις συμβατικές, αλλά δεν συνδέεται με βάση δεδομένων SQL.
2. Wallet Provider: Ο "συνδετικός κρίκος" (π.χ. MetaMask). Το front-end δεν μπορεί να μιλήσει απευθείας στο Blockchain. Χρειάζεται το πορτοφόλι του χρήστη για να υπογράψει κρυπτογραφικά τις συναλλαγές.
3. Smart Contracts (Back-end): Η επιχειρηματική λογική και η βάση δεδομένων ζουν στο Blockchain. Κανείς δεν μπορεί να κατεβάσει τον σέρβερ ή να απαγορεύσει την πρόσβαση σε συγκεκριμένους χρήστες (Censorship Resistance) [41].

6.6.2 DeFi: Οι Χρηματοοικονομικοί "Λίθοι" (Primitives)

Το DeFi δεν είναι απλώς ψηφιακό χρήμα, αλλά ψηφιακή τραπεζική. Οι Werner et al. (2021) κατηγοριοποιούν τις εφαρμογές DeFi σε τέσσερις κύριους πυλώνες:

- Αποκεντρωμένα Ανταλλακτήρια (DEXs): Πλατφόρμες όπως το *Uniswap* χρησιμοποιούν το μοντέλο Automated Market Maker (AMM). Αντί για βιβλίο εντολών (Order Book), οι χρήστες συναλλάσσονται έναντι μιας "δεξαμενής ρευστότητας" (Liquidity Pool) που γεμίζουν άλλοι χρήστες, κερδίζοντας προμήθειες. Η τιμή καθορίζεται αλγοριθμικά (τύπος $x \times y = k$).
- Πρωτόκολλα Δανεισμού (Lending Protocols): Πλατφόρμες όπως το *Aave* επιτρέπουν τον δανεισμό χωρίς πιστοληπτικό έλεγχο. Ο δανεισμός είναι υπερ-καλυμμένος (over-collateralized): για να δανειστείς 100$ σε USDC, πρέπει να κλειδώσεις 150$ σε ETH. Αν η αξία του ETH πέσει, το συμβόλαιο ρευστοποιεί αυτόματα το ενέχυρο.
- Stablecoins: Κρυπτονομίσματα σταθερής ισοτιμίας (peg) με το δολάριο. Διακρίνονται σε κεντρικοποιημένα (USDT, USDC) που βασίζονται σε αποθεματικά τραπεζών, και σε αποκεντρωμένα (DAI) που βασίζονται σε αλγοριθμική διαχείριση ενεχύρων on-chain.

- Yield Farming & Aggregators: Εργαλεία που μετακινούν αυτόματα τα κεφάλαια των χρηστών μεταξύ διαφορετικών πρωτοκόλλων για να μεγιστοποιήσουν την απόδοση (APY), εκμεταλλευόμενα τη συνθεσιμότητα (Composability) του συστήματος [42].

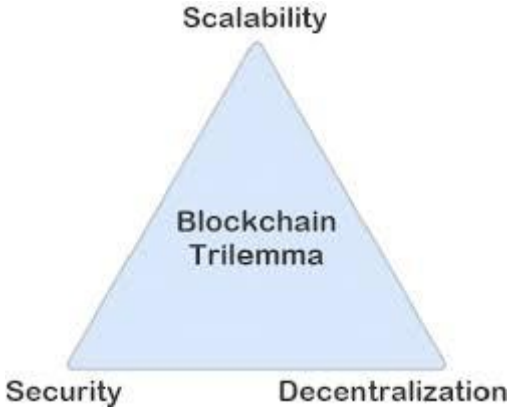
6.6.3 Total Value Locked (TVL) ως Δείκτης Ανάπτυξης: Σε αντίθεση με τις παραδοσιακές εταιρείες που μετρώνται με την κεφαλαιοποίηση (Market Cap), η επιτυχία ενός DApp μετράται με το TVL (Total Value Locked): το συνολικό ποσό κεφαλαίων που έχουν κλειδώσει οι χρήστες στα έξυπνα συμβόλαια του πρωτοκόλλου. Σύμφωνα με μελέτη των Schar (2021), το TVL του DeFi εκτοξεύθηκε από <1 δισ. δολάρια το 2019 σε >100 δισ. το 2021, αποδεικνύοντας την εμπιστοσύνη της αγοράς στον κώδικα έναντι των τραπεζικών ιδρυμάτων [43].

6.6.4 Κίνδυνοι και "Rug Pulls": Η ευκολία δημιουργίας DApps έχει και σκοτεινή πλευρά. Το φαινόμενο "Rug Pull" περιγράφει την περίπτωση όπου οι προγραμματιστές ενός DApp αφαιρούν όλη τη ρευστότητα από το Pool και εξαφανίζονται. Επειδή το DeFi είναι permissionless, δεν υπάρχει ρυθμιστική αρχή για να προστατεύσει τους επενδυτές, καθιστώντας τον έλεγχο του κώδικα (Audit) τη μόνη γραμμή άμυνας.

ΚΕΦΑΛΑΙΟ 7: ΠΡΟΚΛΗΣΕΙΣ ΕΠΕΚΤΑΣΙΜΟΤΗΤΑΣ ΚΑΙ ΛΥΣΕΙΣ ΔΕΥΤΕΡΟΥ ΕΠΙΠΕΔΟΥ (LAYER 2)

7.1 Το Τρίλημμα της Επεκτασιμότητας (The Scalability Trilemma)

Στην επιστήμη των κατανεμημένων συστημάτων, είναι γνωστό ότι δεν υπάρχει "δωρεάν γεύμα". Κάθε αρχιτεκτονική επιλογή συνεπάγεται συγκεκριμένους συμβιβασμούς (trade-offs). Ο Vitalik Buterin, συνιδρυτής του Ethereum, τυποποίησε αυτούς τους περιορισμούς διατυπώνοντας το Τρίλημμα της Επεκτασιμότητας. Το θεώρημα αυτό υποστηρίζει ότι ένα μονολιθικό blockchain δίκτυο μπορεί να βελτιστοποιήσει το πολύ δύο από τις εξής τρεις ιδιότητες: Αποκέντρωση, Ασφάλεια και Επεκτασιμότητα. Η προσπάθεια βελτίωσης της μίας παραμέτρου οδηγεί αναπόφευκτα στην υποβάθμιση τουλάχιστον μίας εκ των άλλων δύο.



Εικόνα 7.1: Το Τρίλημμα της Επεκτασιμότητας του Blockchain και η αδυναμία ταυτόχρονης βελτιστοποίησης των τριών παραμέτρων.

7.1.1 Ανάλυση των Τριών Κορυφών: Για να κατανοήσουμε το πρόβλημα, πρέπει να ορίσουμε αυστηρά τις τρεις παραμέτρους:

Α. Αποκέντρωση (Decentralization) Αφορά τον βαθμό στον οποίο το δίκτυο εξαρτάται από μια κεντρική οντότητα. Ένα αποκεντρωμένο σύστημα επιτρέπει σε οποιονδήποτε χρήστη με βασικό εξοπλισμό (consumer hardware) να τρέξει έναν πλήρη κόμβο (Full Node) και να επαληθεύσει το ιστορικό των συναλλαγών.

- *Ποσοτικοποίηση:* Μετριέται συχνά με τον Συντελεστή Nakamoto (Nakamoto Coefficient), ο οποίος εκφράζει τον ελάχιστο αριθμό οντοτήτων που απαιτούνται για να ελεγχθεί το 51% του δικτύου.
- *Σημασία:* Η αποκέντρωση είναι η μόνη άμυνα ενάντια στη λογοκρισία και τις ρυθμιστικές πιέσεις.

Β. Ασφάλεια (Security) Αναφέρεται στο κόστος που απαιτείται για να παραβιαστεί η ακεραιότητα του καθολικού (Immutability) και να πραγματοποιηθεί μια επίθεση 51% ή μια επίθεση άρνησης υπηρεσίας (DoS).

- *Στο PoW:* Η ασφάλεια εξαρτάται από το συνολικό Hashrate.
- *Στο PoS:* Η ασφάλεια εξαρτάται από την αξία των δεσμευμένων κεφαλαίων (Staked Value).
- *Σχέση με Αποκέντρωση:* Όσο περισσότεροι και ανεξάρτητοι είναι οι κόμβοι, τόσο πιο δύσκολο είναι για έναν επιτιθέμενο να τους συντονίσει ή να τους καταστρέψει.

Γ. Επεκτασιμότητα (Scalability) Είναι η ικανότητα του συστήματος να επεξεργάζεται αυξανόμενο όγκο συναλλαγών χωρίς να αυξάνεται εκθετικά το κόστος ή ο χρόνος επιβεβαίωσης.

- *Throughput:* Ο αριθμός συναλλαγών ανά δευτερόλεπτο (TPS).
- *Latency:* Ο χρόνος μέχρι την οριστικότητα (Time-to-Finality).

7.1.2 Οι Αιτιώδεις Σχέσεις και οι Συμβιβασμοί (Trade-offs): Γιατί δεν μπορούμε να τα έχουμε όλα; Η απάντηση βρίσκεται στους φυσικούς περιορισμούς του υλικού και των δικτύων.

Συμβιβασμός 1: Επεκτασιμότητα εις βάρος της Αποκέντρωσης Για να αυξήσουμε τα TPS (π.χ. όπως κάνει το Solana ή το BSC), πρέπει είτε να αυξήσουμε το μέγεθος του μπλοκ, είτε να μειώσουμε τον χρόνο παραγωγής του. Αυτό όμως απαιτεί:

1. Τεράστια επεξεργαστική ισχύ για την εκτέλεση των συναλλαγών.
2. Τεράστιο bandwidth για τη διάδοση των μπλοκ.
3. Τεράστιο αποθηκευτικό χώρο για το ιστορικό (State Bloat).

Αποτέλεσμα: Οι απλοί χρήστες δεν μπορούν να τρέξουν κόμβους γιατί είναι ακριβό. Το δίκτυο καταλήγει να ελέγχεται από λίγα, βιομηχανικά Data Centers. Το δίκτυο γίνεται γρήγορο, αλλά κεντρικοποιημένο (High Scale, Low Decentralization).

Συμβιβασμός 2: Αποκέντρωση εις βάρος της Επεκτασιμότητας Αυτό είναι το μοντέλο του Bitcoin και του Ethereum (Layer 1). Για να διασφαλιστεί ότι ακόμη και ένας φοιτητής με laptop μπορεί να τρέξει κόμβο, το μέγεθος του μπλοκ διατηρείται τεχνητά μικρό (1MB - 4MB). *Αποτέλεσμα:* Ο καθένας μπορεί να συμμετέχει, η ασφάλεια είναι μέγιστη, αλλά η ταχύτητα είναι εξαιρετικά χαμηλή (Low Scale, High Decentralization).

Συμβιβασμός 3: Ασφάλεια εις βάρος της Αποκέντρωσης Πολλά πρώιμα δίκτυα (Sidechains ή Multi-Sig Bridges) χρησιμοποιούν έναν μικρό αριθμό "έμπιστων" κόμβων (π.χ. 5 κόμβους) για να επικυρώνουν ταχύτατα συναλλαγές. *Αποτέλεσμα:* Το σύστημα είναι γρήγορο, αλλά αν αυτοί οι 5 κόμβοι διαβρωθούν, το δίκτυο καταρρέει (Low Security).

7.1.3 Η Σύνδεση με το Θεώρημα CAP: Το Τρίλημμα του Blockchain αποτελεί ουσιαστικά μια προσαρμογή του Θεωρήματος CAP (Brewer's Theorem) στα οικονομικά δίκτυα. Το CAP ορίζει ότι σε ένα κατανεμημένο σύστημα δεδομένων είναι αδύνατο να εγγυηθείς ταυτόχρονα:

1. Consistency (Συνέπεια): Όλοι οι κόμβοι βλέπουν τα ίδια δεδομένα ταυτόχρονα.
2. Availability (Διαθεσιμότητα): Κάθε αίτημα λαμβάνει απάντηση (όχι σφάλμα).
3. Partition Tolerance (Ανοχή σε Διαμερισμό): Το σύστημα συνεχίζει να λειτουργεί παρά τις διακοπές στο δίκτυο.

Σύμφωνα με τους Brewer (2012) (εδώ μπορείς να βάλεις μια αναφορά σε κλασική βιβλιογραφία CS), τα Blockchains πρέπει υποχρεωτικά να είναι Partition Tolerant (καθώς λειτουργούν στο ανοιχτό Internet). Άρα, πρέπει να επιλέξουν μεταξύ *Άμεσης Συνέπειας* (ασφάλεια/οριστικότητα) και *Διαθεσιμότητας* (ζωντάνια). Το Bitcoin, για παράδειγμα, επιλέγει την Διαθεσιμότητα (Liveness) θυσιάζοντας την άμεση Συνέπεια (επιτρέπει προσωρινά forks), ενώ τα BFT συστήματα (όπως το Cosmos) επιλέγουν τη Συνέπεια (Safety) θυσιάζοντας τη Διαθεσιμότητα (σταματούν αν πέσει το δίκτυο).

7.1.4 Το Κόστος της Επαλήθευσης: Το βαθύτερο πρόβλημα, όπως αναλύουν οι Zhou et al. (2020), είναι ότι στα παραδοσιακά blockchains, κάθε κόμβος πρέπει να επαληθεύσει κάθε συναλλαγή. Δεν υπάρχει καταμερισμός εργασίας. Αυτό δημιουργεί το παράδοξο: *Όσο περισσότεροι κόμβοι μπαίνουν στο δίκτυο, το δίκτυο δεν γίνεται γρηγορότερο, αλλά ασφαλέστερο*. Η ταχύτητα περιορίζεται από τον πιο αδύναμο κόμβο. Για να σπάσει το τρίλημμα, πρέπει να σπάσουμε αυτόν τον κανόνα. Αυτό οδηγεί στις λύσεις Sharding (όπου οι κόμβοι ελέγχουν μόνο τμήμα των συναλλαγών) και Layer 2 (όπου η εκτέλεση βγαίνει εκτός αλυσίδας) [44].

7.2 Λύσεις Πρώτου Επιπέδου (Layer 1 Scaling Solutions)

Οι λύσεις Πρώτου Επιπέδου (On-Chain Scaling) επιχειρούν να αυξήσουν την απόδοση του δικτύου τροποποιώντας τους θεμελιώδεις κανόνες του πρωτοκόλλου. Αυτό απαιτεί συνήθως Hard Fork (μια μη-συμβατή αναβάθμιση που απαιτεί από όλους τους κόμβους να ενημερώσουν το λογισμικό τους). Οι κύριες στρατηγικές εστιάζουν είτε στην αύξηση της χωρητικότητας των μπλοκ, είτε στην παράλληλη επεξεργασία.

7.2.1 Αύξηση Μεγέθους Μπλοκ (Block Size Increase): Η πιο προφανής λύση στο πρόβλημα της επεκτασιμότητας είναι η αύξηση του ορίου δεδομένων ανά μπλοκ.

- Ιστορικό Παράδειγμα (Bitcoin vs Bitcoin Cash): Το 2017, το δίκτυο του Bitcoin διχάστηκε (forked). Η μία πλευρά (Bitcoin Core) επέμεινε στο όριο του 1MB για να διατηρήσει την

αποκέντρωση. Η άλλη πλευρά δημιούργησε το Bitcoin Cash (BCH), αυξάνοντας το όριο στα 8MB (και αργότερα στα 32MB).

- Τεχνικοί Περιορισμοί: Σύμφωνα με τους Zhou et al. (2020), η αύξηση του μεγέθους αυξάνει δραματικά τον Χρόνο Διάδοσης (Propagation Time). Ένα μεγάλο μπλοκ αργεί να ταξιδέψει μέσω του Internet από την Κίνα στις ΗΠΑ. Αυτό αυξάνει τον κίνδυνο των "Ορφανών Μπλοκ" (Orphan/Stale Blocks): δύο miners βρίσκουν μπλοκ ταυτόχρονα, αλλά επειδή το δίκτυο αργεί να ενημερωθεί, η αλυσίδα διασπάται προσωρινά, μειώνοντας την ασφάλεια [44].
- Κίνδυνος Κεντρικοποίησης: Μεγαλύτερα μπλοκ σημαίνουν ότι η αλυσίδα ("Blockchain Size") μεγαλώνει κατά Terabytes τον χρόνο. Μόνο μεγάλα βιομηχανικά κέντρα δεδομένων μπορούν να αποθηκεύσουν το ιστορικό, αποκλείοντας τους ιδιώτες χρήστες.

7.2.2 Segregated Witness (SegWit): και Βελτιστοποίηση Δεδομένων Αντί να αυξήσουμε το μέγεθος του μπλοκ, μπορούμε να κάνουμε τις συναλλαγές μικρότερες. Το Segregated Witness (SegWit), που ενεργοποιήθηκε στο Bitcoin το 2017, διαχωρίζει την κρυπτογραφική υπογραφή (Witness data) από τα δεδομένα της συναλλαγής.

- Μηχανισμός: Οι υπογραφές αποτελούν το ~65% του χώρου μιας συναλλαγής. Με το SegWit, οι υπογραφές μετακινούνται σε μια παράλληλη δομή δεδομένων που δεν μετράει στο όριο του 1MB.
- Αποτέλεσμα: Το "ενεργό" μέγεθος του μπλοκ αυξήθηκε στα ~4MB (block weight), επιτρέποντας 4 φορές περισσότερες συναλλαγές χωρίς Hard Fork.

7.2.3 Sharding (Τεμαχισμός Βάσης Δεδομένων): Το Sharding αποτελεί την "Ιερή Δισκοπότηρο" του Ethereum 2.0. Η ιδέα προέρχεται από τις παραδοσιακές βάσεις δεδομένων: αντί ένας κόμβος να αποθηκεύει όλη τη βάση, αποθηκεύει μόνο ένα κομμάτι της (Shard).

- Οριζόντια Κλιμάκωση (Horizontal Scaling): Το δίκτυο χωρίζεται σε π.χ. 64 Shards. Το Shard 1 επεξεργάζεται συναλλαγές τύπου Α, το Shard 2 τύπου Β, κ.ο.κ. Όλα λειτουργούν παράλληλα.
- Beacon Chain: Είναι ο "μαέστρος" της ορχήστρας. Συντονίζει τα shards, αναθέτει τυχαία validators σε αυτά και καταγράφει τις τελικές καταστάσεις (Cross-links).

Οι Κίνδυνοι του Sharding: Σύμφωνα με τους Hafid et al. (2020), το Sharding εισάγει δύο κρίσιμα προβλήματα:

1. Επίθεση του 1% (Single Shard Attack): Αν το δίκτυο έχει 100 shards, ένας επιτιθέμενος χρειάζεται μόνο το 1% της συνολικής ισχύος για να καταλάβει πλήρως ένα shard και να κλέψει χρήματα από αυτό. *Λύση:* Η Beacon Chain ανακατεύει τυχαία τους validators κάθε λίγα λεπτά, ώστε κανείς να μην μπορεί να προετοιμάσει επίθεση.
2. Δια-τμηματική Επικοινωνία (Cross-Shard Communication): Αν η Alice είναι στο Shard 1 και θέλει να στείλει χρήματα στον Bob στο Shard 2, η διαδικασία είναι αργή και πολύπλοκη, καθώς απαιτείται συγχρονισμός μεταξύ δύο διαφορετικών blockchains [45].

7.2.4 Directed Acyclic Graphs (DAG) - Πέρα από το Blockchain: Μια ριζοσπαστική προσέγγιση Layer 1 είναι η κατάργηση της δομής "αλυσίδας μπλοκ" και η υιοθέτηση της δομής

DAG (Κατευθυνόμενος Ακυκλικός Γράφος). Χρησιμοποιείται από δίκτυα όπως το IOTA (Tangle), το Fantom και το Hedera Hashgraph.

- Λειτουργία: Δεν υπάρχουν μπλοκ και miners. Κάθε χρήστης που θέλει να στείλει μια συναλλαγή, πρέπει να επικυρώσει (μέσω PoW) δύο προηγούμενες συναλλαγές άλλων χρηστών.
- Θεωρητική Κλιμάκωση: Όσο περισσότεροι χρήστες μπαίνουν στο δίκτυο, τόσο πιο γρήγορο γίνεται (το αντίθετο από το Blockchain).
- Μειονέκτημα: Η επίτευξη οριστικότητας (Finality) είναι δύσκολη και συχνά απαιτεί έναν κεντρικό συντονιστή (Coordinator) για την αποφυγή επιθέσεων Double-Spend, μειώνοντας την αποκέντρωση.

7.3 Λύσεις Δεύτερου Επιπέδου (Layer 2 Scaling)

Οι λύσεις Layer 2 χτίζονται *πάνω* στο Blockchain (off-chain scaling). Η ιδέα είναι να μεταφέρουμε το βάρος των υπολογισμών εκτός αλυσίδας και να χρησιμοποιούμε το Layer 1 μόνο για την τελική εκκαθάριση (settlement).

7.3.1 Κανάλια Κατάστασης (State Channels - Lightning Network): Το Lightning Network επιτρέπει σε δύο χρήστες να ανοίξουν ένα ιδιωτικό κανάλι πληρωμών.

1. Κλειδώνουν ένα ποσό στο Bitcoin blockchain (Funding Transaction).
2. Ανταλλάσσουν χιλιάδες συναλλαγές μεταξύ τους off-chain, στιγμιαία και σχεδόν δωρεάν.
3. Όταν τελειώσουν, κλείνουν το κανάλι και γράφουν μόνο το τελικό υπόλοιπο στο Blockchain.

Αποτέλεσμα: Μόνο 2 συναλλαγές γράφονται στο δίκτυο, ενώ πραγματοποιήθηκαν χιλιάδες. Είναι ιδανικό για μικρο-πληρωμές (π.χ. αγορά καφέ).

7.3.2 Rollups: Η Κυρίαρχη Λύση του Ethereum: Τα Rollups "τυλίγουν" εκατοντάδες συναλλαγές σε ένα πακέτο, τις εκτελούν εκτός αλυσίδας και υποβάλλουν μόνο τα συμπιεσμένα δεδομένα (calldata) στο Ethereum. Διακρίνονται σε δύο τύπους:

A. Optimistic Rollups (Optimism, Arbitrum)

- Λειτουργία: Υποθέτουν ότι όλες οι συναλλαγές είναι έγκυρες ("αισιόδοξη" προσέγγιση). Δεν κάνουν κανέναν υπολογισμό on-chain.
- Ασφάλεια: Υπάρχει μια "Περίοδος Αμφισβήτησης" (Challenge Period, συνήθως 7 ημέρες). Αν κάποιος εντοπίσει απάτη, υποβάλλει μια Απόδειξη Απάτης (Fraud Proof). Το δίκτυο ελέγχει την απόδειξη και, αν ισχύει, ακυρώνει τη συναλλαγή και τιμωρεί τον απατεώνα (Slashing).
- Μειονέκτημα: Η ανάληψη κεφαλαίων απαιτεί αναμονή 7 ημερών.

B. ZK-Rollups (Zero-Knowledge Rollups - zkSync, StarkNet)

- Λειτουργία: Χρησιμοποιούν κρυπτογραφικές αποδείξεις μηδενικής γνώσης (Validity Proofs - SNARKs/STARKs). Κάθε πακέτο συναλλαγών συνοδεύεται από μια μαθηματική απόδειξη ότι είναι έγκυρο.

- Πλεονέκτημα: Η εγκυρότητα επιβεβαιώνεται άμεσα. Δεν χρειάζεται περίοδος αναμονής 7 ημερών.
- Μειονέκτημα: Η παραγωγή των αποδείξεων απαιτεί τεράστια υπολογιστική ισχύ.

7.3.3 Η Αρχιτεκτονική των Rollups: Sequencers και Διαθεσιμότητα Δεδομένων:

Η λειτουργία των Rollups δεν είναι μαγική, αλλά βασίζεται σε συγκεκριμένα συστατικά μέρη που εισάγουν νέες έννοιες κεντρικοποίησης και ασφάλειας. Α. Ο Ρόλος του Sequencer (Ακολουθιογράφος) Στα περισσότερα Rollups (όπως το Optimism και το Arbitrum), οι χρήστες δεν στέλνουν τις συναλλαγές τους απευθείας στο Ethereum, αλλά σε έναν ειδικό κόμβο που ονομάζεται Sequencer. Ο Sequencer:

1. Λαμβάνει τις συναλλαγές.
2. Τις διατάσσει (ordering) για να αποτρέψει το Front-running.
3. Τις εκτελεί και παράγει τη νέα κατάσταση (State Root).
4. Υποβάλλει τα δεδομένα στο Layer 1. Σύμφωνα με τους Kogias et al. (2021), αν και το Rollup είναι ασφαλές, ο Sequencer είναι συχνά κεντρικοποιημένος (ελέγχεται από την ομάδα ανάπτυξης). Αν ο Sequencer πέσει, το δίκτυο σταματά (Liveness failure), αν και τα κεφάλαια δεν χάνονται [47].

Β. Το Πρόβλημα της Διαθεσιμότητας Δεδομένων (Data Availability Problem) Για να είναι ασφαλές ένα Rollup, πρέπει οποιοσδήποτε να μπορεί να ανακατασκευάσει την κατάστασή του από το μηδέν. Αυτό σημαίνει ότι τα δεδομένα των συναλλαγών πρέπει να είναι διαθέσιμα δημόσια. Αν ο Sequencer δημοσιεύσει μόνο το hash της νέας κατάστασης (State Root) χωρίς τα δεδομένα που οδήγησαν εκεί, κανείς δεν μπορεί να ελέγξει αν έκανε απάτη. Γι' αυτό, τα Rollups αναγκάζονται να γράφουν συμπιεσμένα δεδομένα στο Ethereum (ως calldata), πληρώνοντας ακριβά τέλη Gas.

ΠΙΝΑΚΑΣ 3: Optimistic vs ZK Rollups

Χαρακτηριστικό	Optimistic Rollups	ZK-Rollups
Βασική Παραδοχή	Οι συναλλαγές θεωρούνται έγκυρες	Απαιτείται κρυπτογραφική απόδειξη
Χρόνος Ανάληψης στο L1	~7 ημέρες (Περίοδος Αμφισβήτησης)	Άμεσος (μόλις επαληθευτεί η απόδειξη)
Υπολογιστικό Κόστος	Πολύ χαμηλό	Πολύ υψηλό (παραγωγή απόδειξης)
Συμβατότητα με EVM	Εξαιρετικά εύκολη	Δύσκολη, αλλά βελτιώνεται (zkEVM)
Τρόπος Επίλυσης Διαφορών	Αποδείξεις Απάτης (Fraud Proofs)	Αποδείξεις Εγκυρότητας (Validity Proofs)

7.4 Sidechains, Γέφυρες και Διαλειτουργικότητα (Interoperability)

Σε ένα πολυ-αλυσιδωτό (multi-chain) μέλλον, όπου το Ethereum, το Solana, το Avalanche και το Bitcoin συνυπάρχουν, η ανάγκη μεταφοράς αξίας και δεδομένων μεταξύ απομονωμένων δικτύων

καθίσταται επιτακτική. Τα Blockchains είναι από τη φύση τους "σιλό": δεν έχουν γνώση για την κατάσταση άλλων δικτύων. Η λύση δίνεται μέσω των Sidechains και των Γεφυρών (Bridges).

7.4.1 Διάκριση Sidechains και Layer 2: Είναι κρίσιμο να διαχωρίσουμε τα Sidechains από τα Rollups (Layer 2), καθώς έχουν διαφορετικό μοντέλο ασφαλείας.

- Layer 2 (Rollups): Κληρονομούν την ασφάλεια του Layer 1. Εάν οι validators του Arbitrum σταματήσουν να λειτουργούν, οι χρήστες μπορούν ακόμα να ανακτήσουν τα κεφάλαιά τους απευθείας από το Ethereum.
- Sidechains (π.χ. Polygon PoS, Ronin): Είναι ανεξάρτητα blockchains με δικό τους μηχανισμό συναίνεσης και δικούς τους validators. Συνδέονται με το κύριο δίκτυο μέσω μιας "αμφίδρομης ζεύξης" (Two-Way Peg).
    - *Κίνδυνος:* Εάν οι validators του Sidechain συνεργαστούν (51% attack), μπορούν να κλέψουν όλα τα κεφάλαια. Το Ethereum δεν μπορεί να κάνει τίποτα για να το αποτρέψει.

7.4.2 Αρχιτεκτονική Γεφυρών: Lock-and-Mint: Ο πιο διαδεδομένος μηχανισμός μεταφοράς tokens μεταξύ αλυσίδων είναι το μοντέλο Lock-and-Mint. Ας υποθέσουμε ότι η Alice θέλει να μεταφέρει 10 ETH από το Ethereum (Source Chain) στο Solana (Destination Chain). Η διαδικασία, σύμφωνα με τους Belchior et al. (2021), έχει ως εξής:

1. Lock (Κλείδωμα): Η Alice στέλνει τα 10 ETH σε ένα Έξυπνο Συμβόλαιο "Θησαυροφυλάκιο" (Vault) στο Ethereum. Τα ETH κλειδώνονται και βγαίνουν εκτός κυκλοφορίας.
2. Verify (Επαλήθευση): Ένας ενδιάμεσος (Oracle ή Validator) παρακολουθεί το Ethereum, βλέπει την κατάθεση και ενημερώνει το Solana.
3. Mint (Δημιουργία): Ένα αντίστοιχο συμβόλαιο στο Solana δημιουργεί (mints) 10 tokens "Wrapped ETH" (wETH), τα οποία έχουν αξία 1:1 με το ETH, και τα στέλνει στο πορτοφόλι της Alice στο Solana.

Για την επιστροφή, ακολουθείται η αντίστροφη διαδικασία Burn-and-Release: Η Alice "καίει" (καταστρέφει) τα wETH στο Solana και το αρχικό συμβόλαιο στο Ethereum "ξεκλειδώνει" τα πραγματικά ETH.

7.4.3 Το Τρίλημμα της Διαλειτουργικότητας: Όπως υπάρχει το Τρίλημμα του Blockchain, έτσι υπάρχει και το Τρίλημμα της Διαλειτουργικότητας, όπως ορίστηκε από τον ιδρυτή του Connext, Arjun Bhuptani. Οι γέφυρες μπορούν να έχουν μόνο δύο από τις εξής τρεις ιδιότητες:

1. Trustlessness (Έλλειψη Εμπιστοσύνης): Η ασφάλεια είναι ίση με αυτή των υποκείμενων blockchains. Δεν χρειάζεται να εμπιστευτούμε τρίτους.
2. Extensibility (Επεκτασιμότητα): Η γέφυρα μπορεί να συνδεθεί εύκολα με οποιοδήποτε δίκτυο (ακόμα και με αυτά που έχουν διαφορετική λογική συναίνεσης).
3. Generalizability (Γενίκευση): Η γέφυρα μπορεί να μεταφέρει οποιοδήποτε είδος δεδομένων (tokens, μηνύματα, εντολές governance).

Οι περισσότερες γέφυρες σήμερα (Multichain, Wormhole) επιλέγουν την Επεκτασιμότητα και τη Γενίκευση, θυσιάζοντας το Trustlessness. Αυτό σημαίνει ότι βασίζονται σε μια μικρή ομάδα επικυρωτών (Multi-Sig), η οποία αποτελεί κεντρικό σημείο αποτυχίας [46].

7.4.4 Μοντέλα Επαλήθευσης και Ασφάλεια: Η ασφάλεια μιας γέφυρας εξαρτάται από το *ποιος* επαληθεύει ότι η κατάθεση στο Source Chain όντως συνέβη. Οι Zamyatin et al. (2021) διακρίνουν τρεις κατηγορίες:

Α. Εξωτερική Επαλήθευση (External Verification - The Multisig Model) Χρησιμοποιείται από τις περισσότερες γέφυρες (Ronin, Wormhole). Υπάρχει μια ομάδα "Φρουρών" (Guardians) εκτός αλυσίδας. Αν οι 5 από τους 8 υπογράψουν ότι είδαν την κατάθεση, η μεταφορά εγκρίνεται.

- *Πλεονέκτημα:* Γρήγορο και φθηνό.
- *Μειονέκτημα:* Εξαιρετικά ευάλωτο. Αν οι hackers κλέψουν τα 5 ιδιωτικά κλειδιά, μπορούν να αδειάσουν το θησαυροφυλάκιο (Honeypot). Αυτό συνέβη στο Ronin Hack ($625M).

Β. Εγγενής Επαλήθευση (Native Verification - Light Clients) Χρησιμοποιείται από το Cosmos IBC και το BTC Relay. Το Destination Chain τρέχει έναν "Light Client" (ελαφρύ κόμβο) του Source Chain μέσα σε ένα έξυπνο συμβόλαιο. Επαληθεύει κρυπτογραφικά τις επικεφαλίδες των μπλοκ (Block Headers).

- *Πλεονέκτημα:* Trustless. Δεν εξαρτάται από τρίτους.
- *Μειονέκτημα:* Πολύ ακριβό σε Gas και δύσκολο να υλοποιηθεί σε ασύμβατες αλυσίδες.

Γ. Τοπική Επαλήθευση (Local Verification - Atomic Swaps) Χρησιμοποιεί τεχνολογία HTLC (όπως το Lightning Network). Οι χρήστες ανταλλάσσουν assets απευθείας (Peer-to-Peer).

- *Πλεονέκτημα:* Απόλυτα ασφαλές.
- *Μειονέκτημα:* Δεν υποστηρίζει γενική μεταφορά μηνυμάτων, παρά μόνο ανταλλαγή νομισμάτων.

7.4.5 Το Πρόβλημα του "Honeypot": Οι γέφυρες δημιουργούν τεράστιες συγκεντρώσεις κεφαλαίων σε ένα σημείο. Όταν η Alice κλειδώνει ETH για να πάει στο Solana, τα ETH μένουν αδρανή στο συμβόλαιο της γέφυρας στο Ethereum. Αν η γέφυρα έχει 1 δισ. δολάρια σε wrapped tokens, σημαίνει ότι το συμβόλαιο στο Ethereum έχει 1 δισ. δολάρια σε πραγματικά assets. Αυτό το καθιστά τον πιο ελκυστικό στόχο για hackers παγκοσμίως. Το 2022 ονομάστηκε "Η χρονιά των Bridge Hacks", με απώλειες άνω των 2 δισ. δολαρίων, αναδεικνύοντας ότι η διαλειτουργικότητα είναι ακόμα ανώριμη τεχνολογικά.

7.5 Αρθρωτά Blockchains (Modular Architecture) και Proto-Danksharding

Η παραδοσιακή αρχιτεκτονική των blockchains, γνωστή ως Μονολιθική (Monolithic), απαιτεί από κάθε κόμβο να επιτελεί ταυτόχρονα τέσσερις λειτουργίες: Εκτέλεση, Διακανονισμό, Συναίνεση και Διαθεσιμότητα Δεδομένων. Αυτό δημιουργεί ένα ανυπέρβλητο εμπόδιο στην κλιμάκωση, καθώς η ταχύτητα του δικτύου περιορίζεται από την επεξεργαστική ισχύ του πιο αδύναμου κόμβου.

Η λύση που προτάθηκε από ερευνητές όπως οι Adler et al. (2022) (Celestia) και υιοθετήθηκε από το Ethereum, είναι η μετάβαση στην Αρθρωτή (Modular) Αρχιτεκτονική. Σε αυτό το μοντέλο, οι λειτουργίες αποσυνδέονται και ανατίθενται σε εξειδικευμένα στρώματα (Layers).

7.5.1 Η Αποσύνθεση των Λειτουργιών: Σύμφωνα με τους Buterin (2022), ένα Blockchain επιτελεί τις εξής διακριτές εργασίες:

1. Εκτέλεση (Execution): Η επεξεργασία των συναλλαγών και η ενημέρωση των υπολοίπων (π.χ. από το Arbitrum/Optimism).
2. Διακανονισμός (Settlement): Η επίλυση διαφορών και η γέφυρα ρευστότητας (π.χ. το Ethereum Mainnet).
3. Συναίνεση (Consensus): Η συμφωνία για τη σειρά των συναλλαγών.
4. Διαθεσιμότητα Δεδομένων (Data Availability - DA): Η εγγύηση ότι τα δεδομένα των συναλλαγών έχουν δημοσιευτεί και είναι προσβάσιμα σε όλους, ώστε να μπορούν να επαληθευτούν.

Στο Modular μοντέλο, το Ethereum μετατρέπεται σταδιακά σε ένα στρώμα που παρέχει *μόνο* Συναίνεση και Διαθεσιμότητα Δεδομένων, αφήνοντας την Εκτέλεση αποκλειστικά στα Rollups (Layer 2).

7.5.2 Το Πρόβλημα της Διαθεσιμότητας Δεδομένων (DA Problem): Γιατί η Διαθεσιμότητα Δεδομένων είναι τόσο κρίσιμη;

Σε ένα Optimistic Rollup, ο Sequencer δημοσιεύει μια "υπόσχεση" (State Root) ότι το αποτέλεσμα των συναλλαγών είναι έγκυρο. Για να μπορέσει ένας παρατηρητής να ελέγξει αν ο Sequencer λέει ψέματα (Fraud Proof), πρέπει να έχει πρόσβαση στα πρωτογενή δεδομένα των συναλλαγών. Αν ο Sequencer αποκρύψει τα δεδομένα (Data Withholding Attack), κανείς δεν μπορεί να αποδείξει την απάτη και τα κεφάλαια κινδυνεύουν.

Μέχρι πρότινος, τα Rollups έγραφαν όλα τα δεδομένα στο Ethereum ως calldata. Επειδή όμως το Ethereum απαιτεί από *όλους* τους κόμβους να κατεβάζουν αυτά τα δεδομένα για πάντα, το κόστος ήταν απαγορευτικό (έως και 90% των τελών Gas πήγαινε στην αποθήκευση).

7.5.3 EIP-4844: Proto-Danksharding και Blobs: Η αναβάθμιση Dencun (EIP-4844), που ενεργοποιήθηκε τον Μάρτιο του 2024, εισήγαγε μια νέα δομή δεδομένων: τα Blobs (Binary Large Objects).

- Προσωρινή Αποθήκευση: Σε αντίθεση με το calldata που μένει για πάντα, τα Blobs αποθηκεύονται στους κόμβους του Ethereum μόνο για ~18 ημέρες (4096 epochs). Αυτός ο χρόνος είναι αρκετός για να ελεγχθεί μια απάτη, αλλά μικρός ώστε να μην επιβαρύνει τον δίσκο των κόμβων.
- Ξεχωριστή Αγορά Τελών (Fee Market): Τα Blobs δεν ανταγωνίζονται τον χώρο των κανονικών συναλλαγών του Ethereum. Έχουν δική τους τιμή Gas (Blob Gas). Αυτό σημαίνει ότι ακόμα και αν το Ethereum "πήξει" από χρήστες που αγοράζουν NFTs, το κόστος των Rollups παραμένει φθηνό.

7.5.4 Κρυπτογραφικές Δεσμεύσεις KZG (Polynomial Commitments)

Πώς εξασφαλίζουμε ότι τα δεδομένα μέσα στο Blob είναι σωστά χωρίς να τα κατεβάσουμε; Εδώ μπαίνουν τα προηγμένα μαθηματικά.

Το EIP-4844 χρησιμοποιεί τις Δεσμεύσεις KZG (Kate-Zaverucha-Goldberg).

- Η Μαθηματική Λογική: Τα δεδομένα ενός Blob μετατρέπονται σε ένα Πολυώνυμο P(x).
- Η Δέσμευση: Ο δημιουργός του Blob παράγει μια μικρή κρυπτογραφική "δέσμευση" $C = g^{P(s)}$ που αντιπροσωπεύει ολόκληρο το πολυώνυμο.
- Η Επαλήθευση: Οποιοσδήποτε κόμβος μπορεί να ελέγξει αν ένα συγκεκριμένο κομμάτι δεδομένων ανήκει στο Blob, χρησιμοποιώντας τη δέσμευση C, χωρίς να χρειάζεται να κατεβάσει ολόκληρο το Blob (μεγέθους 128KB).

Αυτό επιτρέπει στο Ethereum να διαχειρίζεται MBs δεδομένων ανά δευτερόλεπτο, διατηρώντας τους κόμβους ελαφριούς [50].

7.5.5 Data Availability Sampling (DAS): Το Μέλλον: Το επόμενο βήμα μετά το Proto-Danksharding είναι το Full Danksharding. Εδώ εισάγεται η τεχνική DAS.

Αντί οι κόμβοι να κατεβάζουν ολόκληρο το Blob για να βεβαιωθούν ότι είναι διαθέσιμο, κατεβάζουν τυχαία μικρά κομμάτια (samples).

- *Πιθανοτική Εγγύηση:* Αν ένας κόμβος ζητήσει 30 τυχαία δείγματα και τα λάβει όλα, η πιθανότητα να λείπει πάνω από το 50% του Blob (που απαιτείται για την ανακατασκευή του μέσω Erasure Coding) είναι μικρότερη από 10^{-9}.

Αυτό θα επιτρέψει στο Ethereum να επεξεργάζεται εκατομμύρια συναλλαγές το δευτερόλεπτο, καθιστώντας το πραγματικά παγκόσμια υποδομή.

7.6 Πρωτόκολλα Διαλειτουργικότητας και Αρχιτεκτονική Γεφυρών (Cross-Chain Communication)

Σε ένα κατακερματισμένο οικοσύστημα, η αξία και τα δεδομένα παραμένουν εγκλωβισμένα σε μεμονωμένα δίκτυα ("Silos"). Η διαλειτουργικότητα (Interoperability) ορίζεται ως η ικανότητα διαφορετικών blockchains να ανταλλάσσουν πληροφορίες και να εκτελούν συντονισμένες ενέργειες. Σύμφωνα με τους Belchior et al. (2021), η πρόκληση δεν είναι απλώς τεχνική αλλά θεμελιώδης: κάθε blockchain έχει τη δική του έννοια του χρόνου (Finality) και τη δική του κατάσταση (State). Για να επικοινωνήσουν, πρέπει να γεφυρωθεί αυτό το χάσμα συναίνεσης [46].

7.6.1 Ταξινομία Γεφυρών βάσει Μηχανισμού Επαλήθευσης: Η ασφάλεια μιας γέφυρας εξαρτάται αποκλειστικά από το *ποιος* πιστοποιεί ότι μια συναλλαγή συνέβη στην αλυσίδα προέλευσης (Source Chain).

Α. Γέφυρες Εξωτερικής Επαλήθευσης (External Verification - Multisig) Είναι το πιο κοινό και λιγότερο ασφαλές μοντέλο.

- Λειτουργία: Μια ομάδα από επικυρωτές (Validators) παρακολουθεί την αλυσίδα Α. Όταν δουν μια κατάθεση, υπογράφουν ομαδικά (Multisig) μια εντολή για την αλυσίδα Β.

- Κίνδυνος: Οι χρήστες πρέπει να εμπιστεύονται την πλειοψηφία των επικυρωτών. Εάν οι ιδιωτικοί κλειδιά τους κλαπούν (όπως στο Ronin Hack των 625 εκ. δολαρίων), η γέφυρα καταρρέει.
- Παραδείγματα: Multichain, Wormhole, Axie Ronin Bridge.

Β. Γέφυρες Εγγενούς Επαλήθευσης (Native Verification - Light Clients) Είναι το πιο ασφαλές μοντέλο ("Trustless").

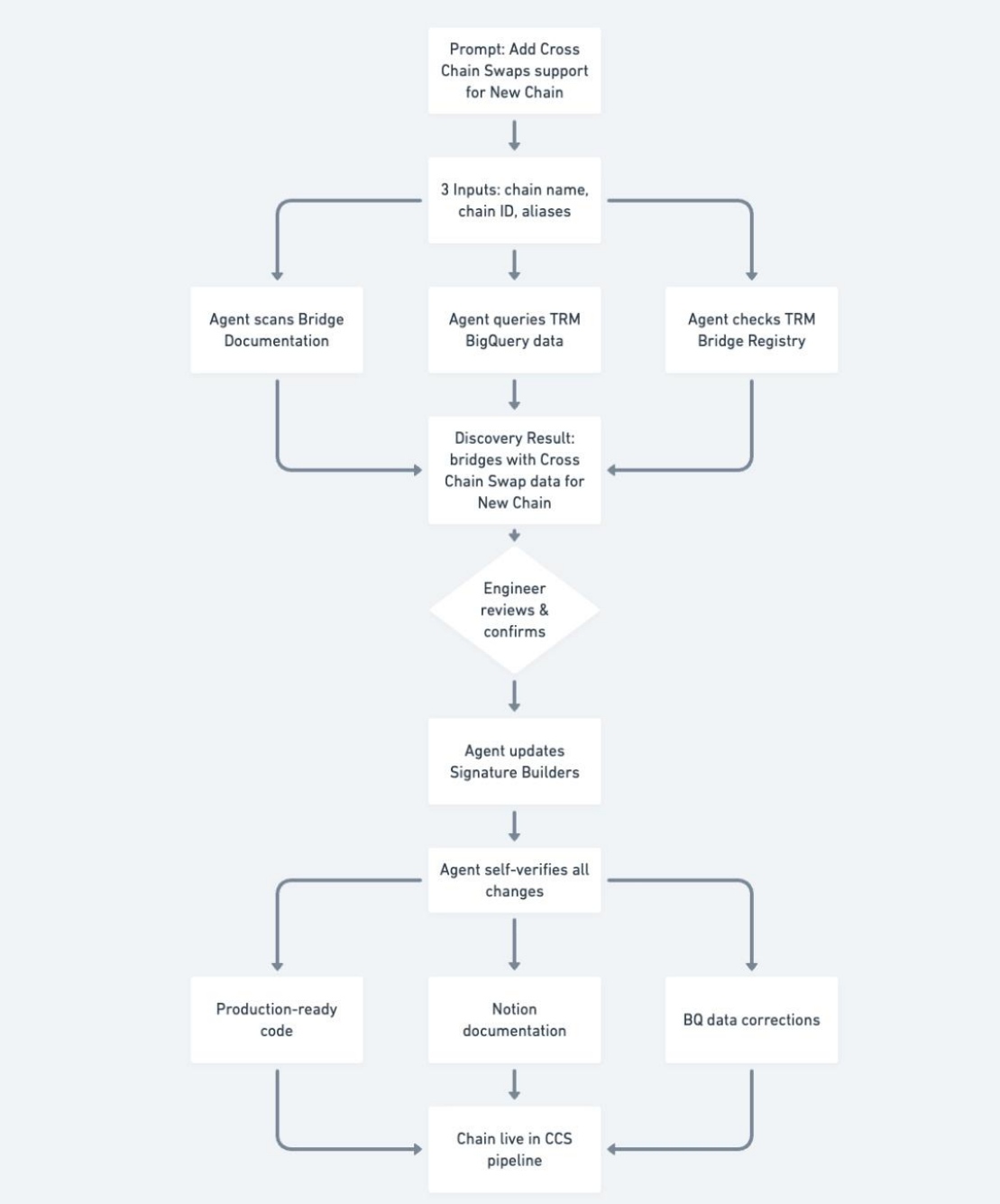
- Λειτουργία: Η αλυσίδα Β τρέχει έναν "Ελαφρύ Κόμβο" (Light Client) της αλυσίδας Α μέσα σε ένα έξυπνο συμβόλαιο. Το συμβόλαιο επαληθεύει κρυπτογραφικά τις επικεφαλίδες των μπλοκ (Block Headers) και τις αποδείξεις Merkle.
- Πλεονέκτημα: Δεν χρειάζεται εμπιστοσύνη σε τρίτους. Η ασφάλεια είναι μαθηματική.
- Μειονέκτημα: Τεράστιο κόστος Gas για την επαλήθευση των υπογραφών εντός του συμβολαίου.
- Παραδείγματα: Cosmos IBC, Near Rainbow Bridge.

Γ. Γέφυρες Τοπικής Επαλήθευσης (Local Verification - Liquidity Networks) Βασίζονται σε ατομικές ανταλλαγές (Atomic Swaps) μεταξύ δύο μερών.

- Λειτουργία: Ο χρήστης δίνει ρευστότητα στην αλυσίδα Α και ένας Liquidity Provider του δίνει ρευστότητα στην αλυσίδα Β.
- Πλεονέκτημα: Ασφαλές, αλλά περιορισμένο μόνο σε μεταφορά tokens (όχι μηνύματα).
- Παραδείγματα: Connext, Hop Protocol.

7.6.2 Lock-and-Mint vs. Burn-and-Redeem: Ο μηχανισμός διαχείρισης των περιουσιακών στοιχείων είναι κρίσιμος για την οικονομική ασφάλεια.

1. Lock-and-Mint: Όταν μεταφέρουμε ETH στο Solana, το ETH κλειδώνεται στο Ethereum και δημιουργείται (mint) ένα "Wrapped Token" (wETH) στο Solana.
    - *Κίνδυνος De-pegging:* Αν το συμβόλαιο στο Ethereum χακαριστεί και αδειάσει, το wETH στο Solana χάνει την αξία του και μηδενίζεται, καθώς δεν υπάρχει πλέον αντίκρισμα.
2. Burn-and-Redeem: Χρησιμοποιείται για νομίσματα που εκδίδονται εγγενώς σε πολλές αλυσίδες (π.χ. USDC με το CCTP της Circle).
    - *Λειτουργία:* Το USDC καίγεται (burn) στο Ethereum και επανεκδίδεται (mint) στο Solana. Δεν υπάρχει "wrapped" έκδοση, άρα δεν υπάρχει κίνδυνος de-pegging.



Εικόνα 7.2: Διαγραμματική απεικόνιση του μηχανισμού Lock-and-Mint για τη μεταφορά ρευστότητας μεταξύ ανεξάρτητων δικτύων.

7.6.3 Γενική Μεταφορά Μηνυμάτων (Arbitrary Message Passing): Η σύγχρονη τάση δεν είναι απλώς η μεταφορά χρημάτων, αλλά η Κλήση Συμβολαίων (Contract Calls) μεταξύ αλυσίδων.

- Παράδειγμα: Ένα DAO στο Ethereum ψηφίζει για να αλλάξει μια παράμετρο σε ένα πρωτόκολλο στο Polygon. Το μήνυμα της ψηφοφορίας ταξιδεύει μέσω της γέφυρας και εκτελείται αυτόματα στον προορισμό.
- Chainlink CCIP (Cross-Chain Interoperability Protocol): Εισάγει ένα πρότυπο ασφαλείας με τρία επίπεδα:
    1. Messaging Router: Δρομολογεί το μήνυμα.
    2. DONs (Decentralized Oracle Networks): Επικυρώνουν το μήνυμα.
    3. Risk Management Network: Ένα ανεξάρτητο δίκτυο που παρακολουθεί για ανωμαλίες και έχει τη δύναμη να "παγώσει" τη γέφυρα σε περίπτωση επίθεσης [51].

7.6.4 ZK-Bridges: Το Μέλλον της Διαλειτουργικότητας: Η χρήση Zero-Knowledge Proofs (ZKPs) λύνει το πρόβλημα κόστους των Light Clients. Αντί το συμβόλαιο στο Ethereum να ελέγχει όλες τις υπογραφές των validators του Solana (που κοστίζει χιλιάδες δολάρια σε Gas), ελέγχει μόνο μία ZK-SNARK απόδειξη.

- Η Απόδειξη: Πιστοποιεί μαθηματικά ότι "οι validators του Solana υπέγραψαν αυτό το μπλοκ και είναι έγκυρο".
- Αποτέλεσμα: Απόλυτη ασφάλεια (Trustless) με ελάχιστο κόστος επαλήθευσης. Εταιρείες όπως η Polyhedra και η Succinct Labs πρωτοπορούν σε αυτόν τον τομέα.

7.6.5 Το Πρωτόκολλο IBC και η Αρχιτεκτονική του Cosmos: Για την αντιμετώπιση των εγγενών αδυναμιών και των κινδύνων που παρουσιάζουν οι παραδοσιακές γέφυρες (όπως το πρόβλημα του "Honeypot" και η ανάγκη εμπιστοσύνης σε κεντρικούς διαμεσολαβητές), αναπτύχθηκαν αρχιτεκτονικές που σχεδιάστηκαν εξ αρχής (ως δίκτυα Layer 0) με αποκλειστικό γνώμονα τη διαλειτουργικότητα. Ο κύριος εκπρόσωπος αυτής της φιλοσοφίας είναι το οικοσύστημα του Cosmos, το οποίο οραματίζεται το «Διαδίκτυο των Blockchains» (Internet of Blockchains).

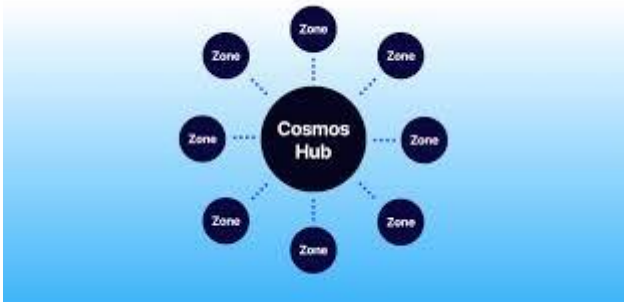
Η αρχιτεκτονική του Cosmos βασίζεται σε μια τοπολογία Κεντρικού Κόμβου και Ζωνών (Hub and Zones). Κάθε «Ζώνη» (Zone) αποτελεί ένα απολύτως ανεξάρτητο και κυρίαρχο (sovereign) Blockchain (Application-Specific Blockchain). Κάθε Ζώνη διατηρεί τον δικό της μηχανισμό συναίνεσης, συνήθως βασισμένο στον αλγόριθμο Tendermint BFT, και τους δικούς της επικυρωτές (validators). Συνεπώς, κάθε Ζώνη είναι αποκλειστικά υπεύθυνη για τη δική της ασφάλεια. Για να αποφευχθεί η πολυπλοκότητα της σύνδεσης κάθε Ζώνης με όλες τις υπόλοιπες, όλες οι Ζώνες συνδέονται ακτινωτά με έναν κεντρικό δρομολογητή, το Cosmos Hub.

Ο ακρογωνιαίος λίθος αυτού του συστήματος είναι το πρωτόκολλο Δια-Αλυσιδωτής Επικοινωνίας (Inter-Blockchain Communication - IBC). Το IBC αποτελεί ένα τυποποιημένο πλαίσιο επικοινωνίας που συχνά παρομοιάζεται με το πρωτόκολλο TCP/IP του παραδοσιακού διαδικτύου. Η λειτουργία του βασίζεται σε τρία βασικά στοιχεία:

1. Ελαφρείς Πελάτες (Light Clients): Το Blockchain A διατηρεί έναν ελαφρύ κόμβο του Blockchain B εντός του δικού του κώδικα, παρακολουθώντας συνεχώς τις επικεφαλίδες των μπλοκ (block headers) του B, και αντίστροφα. Αυτό επιτρέπει την κρυπτογραφική επαλήθευση της κατάστασης χωρίς την ανάγκη τρίτων μερών.
2. Αναμεταδότες (Relayers): Επειδή τα blockchains δεν μπορούν να στείλουν δεδομένα μόνα τους στον έξω κόσμο, ειδικοί κόμβοι (Relayers) σαρώνουν (scan) τις αλυσίδες για

πακέτα IBC. Μόλις εντοπίσουν ένα εξερχόμενο πακέτο στην αλυσίδα Α, το "πακετάρουν" σε μια συναλλαγή και το υποβάλλουν στην αλυσίδα Β.

3. Άμεση Οριστικότητα (Instant Finality): Το IBC απαιτεί οι αλυσίδες που συνδέονται να έχουν άμεση οριστικότητα (όπως προσφέρει το Tendermint). Αν μια αλυσίδα έχει πιθανοτική οριστικότητα (όπως το Bitcoin ή το Ethereum), απαιτείται η χρήση ειδικών "Peg-Zones" που λειτουργούν ως μεταφραστές οριστικότητας.



Εικόνα 7.3: Η αρχιτεκτονική "Κεντρικού Κόμβου και Ζωνών" (Hub and Zones) του οικοσυστήματος Cosmos.

7.6.6 Η Αρχιτεκτονική «Κοινόχρηστης Ασφάλειας» του Polkadot: Μια εντελώς διαφορετική προσέγγιση στο πρόβλημα της διαλειτουργικότητας και του κατακερματισμού προσφέρει το οικοσύστημα του Polkadot. Αντί να συνδέει ανεξάρτητα και κυρίαρχα δίκτυα όπως το Cosmos, το Polkadot λειτουργεί ως ένα ετερογενές πολυ-αλυσιδωτό πλαίσιο (heterogeneous multi-chain framework).

Στην καρδιά του συστήματος βρίσκεται η Αλυσίδα Αναμετάδοσης (Relay Chain), η οποία λειτουργεί ως το θεμέλιο Layer 0. Το μοναδικό χαρακτηριστικό της Relay Chain είναι ότι δεν υποστηρίζει έξυπνα συμβόλαια ούτε εκτελεί εφαρμογές. Ο μοναδικός της ρόλος είναι να παρέχει ασφάλεια, συναίνεση και δρομολόγηση μηνυμάτων. Γύρω από την κεντρική αλυσίδα συνδέονται οι Παρα-αλυσίδες (Parachains), οι οποίες είναι εξειδικευμένα δίκτυα Layer 1, βελτιστοποιημένα για διαφορετικές χρήσεις (π.χ. DeFi, Gaming, IoT).

Η θεμελιώδης καινοτομία και η μεγαλύτερη διαφορά του Polkadot από το Cosmos είναι η «Κοινόχρηστη Ασφάλεια» (Shared Security). Στο μοντέλο του Cosmos, εάν μια μικρή Ζώνη έχει χαμηλή κεφαλαιοποίηση, ένας επιτιθέμενος μπορεί εύκολα να αγοράσει το 51% των νομισμάτων της και να την παραβιάσει. Στο Polkadot, οι Parachains δεν έχουν δικούς τους επικυρωτές. Η παραγωγή των μπλοκ γίνεται από εξειδικευμένους κόμβους (Collators) που ανήκουν στην Parachain, αλλά η τελική επικύρωση και ενσωμάτωσή τους στο παγκόσμιο ιστορικό γίνεται αποκλειστικά από τους Επικυρωτές (Validators) της κεντρικής Relay Chain.

Αυτό σημαίνει ότι για να επιτεθεί κάποιος σε μια μικρή Parachain, πρέπει να επιτεθεί σε ολόκληρο το δίκτυο του Polkadot, εγγυώμενος έτσι ομοιόμορφη ασφάλεια (uniform security) σε όλο το οικοσύστημα. Η διαλειτουργικότητα επιτυγχάνεται εγγενώς μέσω του εσωτερικού πρωτοκόλλου XCM (Cross-Consensus Message Format), το οποίο επιτρέπει όχι μόνο τη μεταφορά νομισμάτων, αλλά την αποστολή αυθαίρετων μηνυμάτων και εντολών μεταξύ των Parachains με μαθηματική βεβαιότητα.

ΚΕΦΑΛΑΙΟ 8: ΨΗΦΙΑΚΗ ΤΑΥΤΟΤΗΤΑ, ΤΟΚΕΝΟΠΟΙΗΣΗ ΚΑΙ Η ΟΙΚΟΝΟΜΙΑ ΤΩΝ ΠΡΑΓΜΑΤΙΚΩΝ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ (RWA)

8.1 Τοκενοποίηση Περιουσιακών Στοιχείων (Real World Assets - RWA)

Η τοκενοποίηση (Tokenization) ορίζεται ως η διαδικασία ψηφιακής αναπαράστασης δικαιωμάτων ιδιοκτησίας υλικών ή άυλων περιουσιακών στοιχείων σε ένα κατανεμημένο καθολικό (DLT). Δεν πρόκειται απλώς για την εγγραφή δεδομένων σε μια βάση, αλλά για τη δημιουργία ενός προγραμματιζόμενου "έξυπνου τίτλου" που αλληλεπιδρά αυτόματα με το χρηματοπιστωτικό σύστημα. Σύμφωνα με την έκθεση της Citigroup (2023), η αγορά των RWA αναμένεται να αγγίξει τα 5 τρισεκατομμύρια δολάρια έως το 2030, οδηγούμενη κυρίως από την ανάγκη για ρευστότητα σε παραδοσιακά "δυσκίνητες" αγορές [54].

8.1.1 Ταξινομία: Native vs. Non-Native RWAs: Η ακαδημαϊκή κοινότητα διακρίνει τα RWA σε δύο κατηγορίες:

1. Non-Native RWAs (Μη-Εγγενή): Περιουσιακά στοιχεία που υπάρχουν στον φυσικό κόσμο (π.χ. ακίνητα, ράβδοι χρυσού, μετοχές της Apple). Το token λειτουργεί ως "ψηφιακό είδωλο" (digital twin) και η αξία του εξαρτάται από τη νομική επιβολή (legal enforceability) της σύνδεσης μεταξύ του token και του φυσικού αντικειμένου.
2. Native RWAs (Εγγενή): Περιουσιακά στοιχεία που δημιουργούνται απευθείας στο Blockchain (π.χ. ψηφιακά ομόλογα που εκδίδονται από την Ευρωπαϊκή Τράπεζα Επενδύσεων στο Ethereum). Εδώ, το token *είναι* το περιουσιακό στοιχείο, όχι απλώς η αναπαράστασή του.

8.1.2 Τεχνικά Πρότυπα Ασφαλείας: ERC-1400 και ERC-3643: Ενώ τα ERC-20 tokens είναι ανώνυμα και ελεύθερα μεταβιβάσιμα, τα RWA απαιτούν αυστηρή συμμόρφωση (Compliance).

Α. ERC-1400 (The Security Token Standard) Είναι ένα πιο σύνθετο πρότυπο που εισάγει την έννοια των Partitions (Τμημάτων).

- Επιτρέπει στο ίδιο token να έχει διαφορετικές καταστάσεις. Παράδειγμα: Μια εταιρεία εκδίδει μετοχές. Κάποιες είναι "Common Shares" (με δικαίωμα ψήφου) και κάποιες "Preferred Shares" (με προτεραιότητα στο μέρισμα). Το ERC-1400 διαχειρίζεται αυτές τις διαφορές μέσα στο ίδιο έξυπνο συμβόλαιο.
- Υποστηρίζει Operator Control: Σε περίπτωση απώλειας κλειδιών ή δικαστικής εντολής, ο διαχειριστής (Issuer) μπορεί να "εξαναγκάσει" τη μεταφορά tokens (force transfer), κάτι που απαγορεύεται στο Bitcoin/Ethereum αλλά είναι υποχρεωτικό στις κεφαλαιαγορές.

Β. ERC-3643 (T-REX Protocol - Token for Regulated Exchanges) Εστιάζει στην ψηφιακή ταυτότητα. Χρησιμοποιεί ένα σύστημα ONCHAINID, όπου κάθε επενδυτής έχει μια επαληθευμένη ταυτότητα στο Blockchain. Το token ελέγχει αυτόματα:

1. Είναι ο παραλήπτης στη Whitelist;
2. Έχει λήξει η περίοδος υποχρεωτικής διακράτησης (Lock-up period);
3. Έχει ο παραλήπτης υπερβεί το όριο επένδυσης ανά έτος; Αν οποιοσδήποτε έλεγχος αποτύχει, η συναλλαγή απορρίπτεται σε επίπεδο πρωτοκόλλου.

8.1.3 Διαφάνεια και Αποτίμηση: Chainlink Proof of Reserve (PoR): Ένα κρίσιμο πρόβλημα στα RWA είναι η εμπιστοσύνη. Πώς γνωρίζει ο επενδυτής ότι το token "Gold-Token" καλύπτεται πραγματικά από ράβδους χρυσού σε ένα θησαυροφυλάκιο στην Ελβετία; Η λύση είναι οι Χρησμοί (Oracles) τύπου Proof of Reserve.

- Λειτουργία: Ένας ελεγκτής (Auditor) ελέγχει το θησαυροφυλάκιο και δημοσιεύει τα δεδομένα σε ένα API.
- Oracle Network: Το Chainlink αντλεί αυτά τα δεδομένα, τα επαληθεύει και τα ενημερώνει στο έξυπνο συμβόλαιο.
- Circuit Breaker: Εάν η αξία των tokens ξεπεράσει την αξία του φυσικού αποθέματος (under-collateralization), το έξυπνο συμβόλαιο παγώνει αυτόματα τη δημιουργία νέων tokens για να αποτρέψει την απάτη [60].

8.1.4 Διαχείριση Κύκλου Ζωής (Corporate Actions): Η τοκενοποίηση δεν αφορά μόνο την πώληση, αλλά και τη διαχείριση του τίτλου (Lifecycle Management).

- Διανομή Μερισμάτων (Dividends): Αντί να στέλνονται επιταγές ή εμβάσματα σε 1.000 μετόχους, το έξυπνο συμβόλαιο λαμβάνει USDC και το μοιράζει αυτόματα σε όλους τους κατόχους του token (airdrop) αναλογικά με το ποσοστό τους, μέσα σε δευτερόλεπτα.
- Ψηφοφορία (Voting): Οι κάτοχοι tokens ψηφίζουν για εταιρικές αποφάσεις (Governance) απευθείας μέσω του ψηφιακού τους πορτοφολιού, με τα αποτελέσματα να είναι αδιάβλητα και άμεσα επαληθεύσιμα.

8.1.5 Μελέτη Περίπτωσης: Ιδιωτική Πίστωση (Private Credit) και Centrifuge Ένα από τα πιο επιτυχημένα παραδείγματα RWA είναι η πλατφόρμα Centrifuge.

- Το Πρόβλημα: Οι Μικρομεσαίες Επιχειρήσεις (SMEs) δυσκολεύονται να πάρουν δάνεια από τράπεζες.
- Η Λύση: Μια επιχείρηση "τοκενοποιεί" τα απλήρωτα τιμολόγιά της (Invoices) ως NFTs.
- Η Διαδικασία:
    1. Η εταιρεία ανεβάζει το τιμολόγιο και δημιουργεί ένα NFT.
    2. Καταθέτει το NFT σε μια δεξαμενή ρευστότητας (Pool) στο Centrifuge.
    3. Επενδυτές DeFi καταθέτουν Stablecoins (DAI) στη δεξαμενή για να κερδίσουν τόκο.
    4. Η εταιρεία δανείζεται τα DAI έναντι του NFT. Όταν ο πελάτης πληρώσει το τιμολόγιο, η εταιρεία αποπληρώνει το δάνειο + τόκους. Αυτό επιτρέπει τη ροή κεφαλαίων από το DeFi στην πραγματική οικονομία, παρακάμπτοντας το τραπεζικό σύστημα [61].

8.2 Το Ευρωπαϊκό Ρυθμιστικό Πλαίσιο MiCA και η Κανονιστική Συμμόρφωση

Η ψήφιση του Κανονισμού (ΕΕ) 2023/1114 για τις αγορές κρυπτοστοιχείων, γνωστού ως MiCA, σηματοδοτεί το τέλος της εποχής της "Άγριας Δύσης" για τα ψηφιακά περιουσιακά στοιχεία. Η Ευρωπαϊκή Ένωση είναι η πρώτη μεγάλη δικαιοδοσία παγκοσμίως που εισάγει ένα ολοκληρωμένο νομικό πλαίσιο, προσφέροντας νομική σαφήνεια που λείπει από τις ΗΠΑ (όπου επικρατεί η "ρύθμιση μέσω επιβολής" από την SEC). Σύμφωνα με την ανάλυση των Zetzsche et al. (2021), ο MiCA έχει διττό στόχο: την προστασία των καταναλωτών από απάτες (τύπου FTX) και την ενίσχυση της καινοτομίας μέσω της νομικής ασφάλειας για τους θεσμικούς επενδυτές [63].

8.2.1 Η Ταξινόμηση των Κρυπτοστοιχείων (Token Taxonomy): Ο MiCA δεν αντιμετωπίζει όλα τα tokens με τον ίδιο τρόπο. Εισάγει τρεις διακριτές κατηγορίες, καθεμία με διαφορετικές απαιτήσεις:

Α. E-Money Tokens (EMTs) Πρόκειται για τα γνωστά μας Stablecoins που αναφέρονται σε ένα μόνο επίσημο νόμισμα (π.χ. USDC, Euro Coin).

- Απαίτηση: Μπορούν να εκδίδονται μόνο από Πιστωτικά Ιδρύματα (Τράπεζες) ή Ιδρύματα Ηλεκτρονικού Χρήματος (EMIs).
- Ρευστότητα: Ο εκδότης πρέπει να διατηρεί αποθεματικά 1:1 σε μετρητά ή ισοδύναμα μετρητών.
- Δικαίωμα Εξαργύρωσης: Ο κάτοχος του token έχει νομικό δικαίωμα (claim) να ζητήσει την εξαργύρωση ανά πάσα στιγμή στην ονομαστική αξία (at par).

Β. Asset-Referenced Tokens (ARTs) Αυτά είναι tokens που αναφέρονται σε ένα "καλάθι" νομισμάτων, εμπορευμάτων ή άλλων κρυπτοστοιχείων για να διατηρήσουν σταθερή αξία (π.χ. το αρχικό σχέδιο του Libra/Diem του Facebook).

- Κίνδυνος: Θεωρούνται συστημικός κίνδυνος για τη νομισματική κυριαρχία του Ευρώ.
- Περιορισμοί: Αν οι συναλλαγές ARTs ξεπεράσουν το 1 εκατ. την ημέρα ή τα 200 εκατ. ευρώ σε αξία, η ΕΚΤ μπορεί να σταματήσει την έκδοσή τους.

Γ. Utility Tokens και Άλλα Κρυπτοστοιχεία Εδώ εντάσσονται τα περισσότερα κρυπτονομίσματα (π.χ. Bitcoin, Ether, Governance tokens) που δεν είναι stablecoins.

- Υποχρέωση: Οι εκδότες (αν υπάρχουν, π.χ. για ICOs) πρέπει να δημοσιεύουν Λευκή Βίβλο (Whitepaper) με συγκεκριμένη δομή, αναφέροντας ρητά τους κινδύνους και την τεχνολογία.

8.2.2 Πάροχοι Υπηρεσιών Κρυπτοστοιχείων (CASPs): Ο MiCA ρυθμίζει αυστηρά τους ενδιάμεσους, ονομάζοντάς τους Crypto-Asset Service Providers (CASPs). Σε αυτή την κατηγορία ανήκουν τα Ανταλλακτήρια (Exchanges), οι Θεματοφύλακες (Custodians) και οι Σύμβουλοι Επενδύσεων. Οι υποχρεώσεις τους είναι βαρύτατες:

1. Φυσική Παρουσία: Πρέπει να έχουν έδρα σε κράτος-μέλος της ΕΕ και να λάβουν άδεια λειτουργίας από την εθνική αρχή (π.χ. Επιτροπή Κεφαλαιαγοράς).
2. Διαχωρισμός Κεφαλαίων (Segregation of Funds): Απαγορεύεται αυστηρά η ανάμειξη των κεφαλαίων των πελατών με τα κεφαλαία της εταιρείας. Αυτό έγινε για να αποτραπεί μια νέα περίπτωση FTX, όπου το ανταλλακτήριο τζόγαρε τα χρήματα των πελατών.

3. Ευθύνη για Hacks: Εάν ένας Θεματοφύλακας χάσει τα κρυπτοστοιχεία των πελατών λόγω κυβερνοεπίθεσης ή δυσλειτουργίας, υποχρεούται να τα αποζημιώσει, εκτός αν αποδείξει ότι το γεγονός ήταν εκτός ελέγχου του.

8.2.3 Ο "Ταξιδιωτικός Κανόνας" (The Travel Rule - TFR): Παράλληλα με τον MiCA, ψηφίστηκε ο Κανονισμός για τη Μεταφορά Κεφαλαίων (Transfer of Funds Regulation - TFR), που στοχεύει στο Ξέπλυμα Χρήματος (AML).

- Η Απαίτηση: Κάθε φορά που ένα ανταλλακτήριο (CASP A) στέλνει κρυπτοστοιχεία σε ένα άλλο ανταλλακτήριο (CASP B), πρέπει να διαβιβάζει ταυτόχρονα και τα προσωπικά στοιχεία του αποστολέα και του παραλήπτη (Όνομα, Διεύθυνση, Αριθμό Ταυτότητας), όπως κάνουν οι τράπεζες με το SWIFT.
- Unhosted Wallets: Εάν η μεταφορά γίνεται προς ιδιωτικό πορτοφόλι (π.χ. Ledger) και το ποσό υπερβαίνει τα €1.000, το ανταλλακτήριο πρέπει να επαληθεύσει ότι το πορτοφόλι ανήκει όντως στον πελάτη του (Proof of Ownership).

8.2.4 Κατάχρηση Αγοράς (Market Abuse): Για πρώτη φορά, θεσπίζονται κανόνες κατά της χειραγώγησης της αγοράς στα κρυπτονομίσματα.

- Insider Trading: Απαγορεύεται η χρήση προνομιακών πληροφοριών για αποκόμιση κέρδους (π.χ. ένας υπάλληλος ανταλλακτηρίου που αγοράζει ένα token πριν αυτό εισαχθεί στην πλατφόρμα).
- Market Manipulation: Απαγορεύονται πρακτικές όπως το "Wash Trading" (ψεύτικος όγκος συναλλαγών) και το "Pump and Dump" μέσω influencers.

8.2.5 Τι μένει εκτός (DeFi και NFTs): Είναι σημαντικό να σημειωθεί ότι ο MiCA εξαιρεί προσωρινά τα πλήρως αποκεντρωμένα πρωτόκολλα (DeFi) και τα πραγματικά μοναδικά NFTs (όχι συλλογές τύπου 10.000 Bored Apes που θεωρούνται επενδυτικά προϊόντα). Η Ευρωπαϊκή Επιτροπή ετοιμάζει ξεχωριστή έκθεση για το πώς θα ρυθμιστεί το DeFi (Embedded Supervision) έως το 2025.

8.3 Ψηφιακά Νομίσματα Κεντρικών Τραπεζών (Central Bank Digital Currencies - CBDCs)

Τα CBDC ορίζονται ως μια ψηφιακή μορφή χρήματος κεντρικής τράπεζας που διατίθεται στο ευρύ κοινό. Διαφέρουν θεμελιωδώς από τα αποθεματικά που διατηρούν οι εμπορικές τράπεζες στην κεντρική τράπεζα, καθώς είναι καθολικά προσβάσιμα. Σύμφωνα με την Τράπεζα Διεθνών Διακανονισμών (BIS, 2023), πάνω από το 93% των κεντρικών τραπεζών παγκοσμίως διερευνούν ή αναπτύσσουν CBDCs, με στόχο τη διασφάλιση της νομισματικής κυριαρχίας απέναντι στα Stablecoins και τα Big Tech νομίσματα (π.χ. το ακυρωθέν Libra του Facebook) [55].

Εικόνα 8.1: Συγκριτική απεικόνιση των αρχιτεκτονικών μοντέλων Χονδρικής (Wholesale) και Λιανικής (Retail) για τα Νομίσματα Κεντρικών Τραπεζών (CBDCs).

8.3.1 Το Μοντέλο Δύο Επιπέδων (Two-Tier / Hybrid Model): Η μεγαλύτερη ανησυχία για τα CBDCs είναι η αποσταθεροποίηση του τραπεζικού συστήματος (Banking Disintermediation). Εάν οι πολίτες μπορούσαν να ανοίξουν λογαριασμό απευθείας στην ΕΚΤ ή τη Fed, θα απέσυραν τις καταθέσεις τους από τις εμπορικές τράπεζες σε περιόδους κρίσης, προκαλώντας Bank Runs. Για να αποφευχθεί αυτό, έχει επιλεγεί σχεδόν καθολικά το Υβριδικό Μοντέλο:

- Επίπεδο 1 (Κεντρική Τράπεζα): Εκδίδει το CBDC και διαχειρίζεται το κεντρικό καθολικό (Wholesale Ledger). Διασφαλίζει την ακεραιότητα της προσφοράς χρήματος.
- Επίπεδο 2 (Ενδιάμεσοι - PSPs): Τράπεζες και εταιρείες Fintech αναλαμβάνουν τη διανομή, το KYC (Know Your Customer) και την ανάπτυξη των ψηφιακών πορτοφολιών. Η Κεντρική Τράπεζα δεν έχει άμεση επαφή με τους τελικούς χρήστες και δεν βλέπει τα προσωπικά τους δεδομένα.

8.3.2 Τεχνολογία: DLT ή Κεντρική Βάση Δεδομένων; Ένα συχνό ερώτημα είναι αν τα CBDC χρειάζονται Blockchain. Η απάντηση είναι: *Όχι απαραίτητα, αλλά το DLT προσφέρει πλεονεκτήματα*.

- Project Hamilton (Fed & MIT): Σε πειράματα της Ομοσπονδιακής Τράπεζας της Βοστώνης, αποδείχθηκε ότι μια καλά σχεδιασμένη κεντρική βάση δεδομένων μπορεί να επεξεργαστεί 1,7 εκατομμύρια συναλλαγές το δευτερόλεπτο (TPS), πολύ περισσότερες από οποιοδήποτε Blockchain.
- Γιατί DLT; Πολλές τράπεζες (π.χ. Banque de France) επιλέγουν DLT (συνήθως Permissioned εκδοχές του Ethereum ή το Corda) για να εκμεταλλευτούν τα Έξυπνα Συμβόλαια και την Ατομικότητα (Atomicity). Αυτό επιτρέπει το λεγόμενο Delivery-versus-Payment (DvP): το ομόλογο μεταβιβάζεται *μόνο αν* πληρωθεί το CBDC, εξαλείφοντας τον κίνδυνο αθέτησης (counterparty risk) [65].

8.3.3 Διασυνοριακές Πληρωμές: Project mBridge: Το σημερινό σύστημα SWIFT είναι αργό και ακριβό γιατί βασίζεται σε αλυσίδες ανταποκριτριών τραπεζών (Correspondent Banking). Το CBDC υπόσχεται να το αλλάξει αυτό. Το Project mBridge (συνεργασία BIS, Κίνας, ΗΑΕ, Ταϊλάνδης) χρησιμοποιεί ένα κοινό Blockchain ("mBridge Ledger") όπου διαφορετικές κεντρικές τράπεζες εκδίδουν τα νομίσματά τους.

- Αποτέλεσμα: Μια πληρωμή από το Πεκίνο στο Ντουμπάι γίνεται σε δευτερόλεπτα (αντί για μέρες), απευθείας Peer-to-Peer μεταξύ των τραπεζών, παρακάμπτοντας το δολάριο και το αμερικανικό τραπεζικό σύστημα. Αυτό έχει τεράστιες γεωπολιτικές προεκτάσεις.

8.3.4 Προγραμματιζόμενο Χρήμα και Ιδιωτικότητα: Η πιο αμφιλεγόμενη πτυχή των CBDCs είναι η δυνατότητα προγραμματισμού (Programmability).

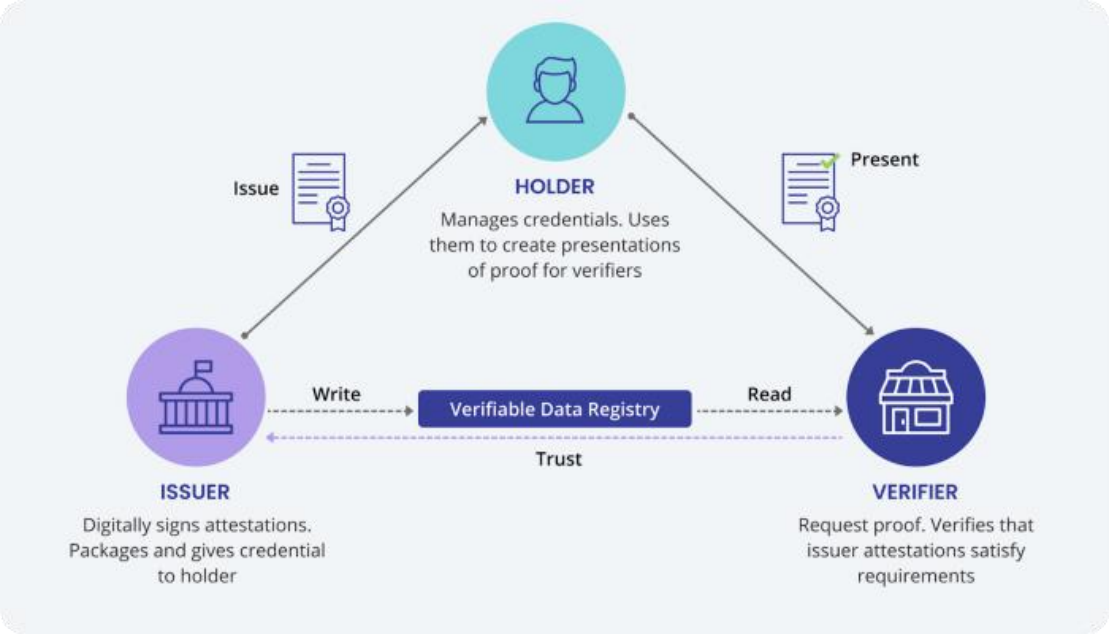
- Θετική Όψη: Το κράτος θα μπορούσε να στείλει επιδόματα που μπορούν να ξοδευτούν *μόνο* για τρόφιμα ή ενέργεια, ή χρήματα που λήγουν αν δεν ξοδευτούν (για τόνωση της κατανάλωσης).
- Αρνητική Όψη (Δυστοπία): Η Κεντρική Τράπεζα θα μπορούσε τεχνικά να "παγώσει" τα χρήματα διαφωνούντων πολιτών ή να επιβάλει αρνητικά επιτόκια απευθείας στο πορτοφόλι του πολίτη.
- Η Λύση της Τεχνολογίας: Για να διασκεδαστούν οι ανησυχίες, το Ψηφιακό Ευρώ σχεδιάζεται με τεχνολογία "Cash-like Privacy" για μικροποσά. Επίσης, ερευνητικά έργα όπως το Project Tourbillon χρησιμοποιούν Zero-Knowledge Proofs για να κρύψουν τα ποσά των συναλλαγών από την Κεντρική Τράπεζα, επιτρέποντας μόνο τον έλεγχο ότι "ο χρήστης δεν ξόδεψε τα ίδια χρήματα δύο φορές" (Double-spending check) [66].

8.3.5 Offline Πληρωμές (Offline Capability): Ένα CBDC πρέπει να λειτουργεί ακόμα και όταν πέσει το Internet ή το ρεύμα (κάτι που τα κρυπτονομίσματα δυσκολεύονται να κάνουν). Η τεχνική λύση βασίζεται στο Secure Element (SE) των κινητών τηλεφώνων (το τσιπάκι που χρησιμοποιείται για το Apple Pay) ή σε έξυπνες κάρτες.

- Λειτουργία: Η αξία αποθηκεύεται τοπικά στο hardware. Όταν δύο συσκευές ακουμπήσουν (μέσω NFC), τα χρήματα μεταφέρονται από το ένα τσιπ στο άλλο χωρίς να μιλήσουν με κανέναν server. Το Secure Element εγγυάται ότι τα χρήματα αφαιρέθηκαν από τον αποστολέα.

8.4 Αυτοκυρίαρχη Ταυτότητα (Self-Sovereign Identity - SSI)

Το σημερινό μοντέλο ψηφιακής ταυτότητας είναι "Φεουδαρχικό". Οι ψηφιακοί μας εαυτοί ανήκουν σε εταιρικούς κολοσσούς (Google, Facebook, Apple), οι οποίοι λειτουργούν ως "Πάροχοι Ταυτότητας" (Identity Providers). Αν η Google κλείσει τον λογαριασμό ενός χρήστη, αυτός χάνει την πρόσβαση σε δεκάδες συνδεδεμένες υπηρεσίες. Το Web3 εισάγει το παράδειγμα της Αυτοκυρίαρχης Ταυτότητας (SSI): ο χρήστης είναι ο αποκλειστικός ιδιοκτήτης και διαχειριστής των δεδομένων του, χωρίς να εξαρτάται από κανέναν ενδιάμεσο.



Εικόνα 8.2: Το «Τρίγωνο Εμπιστοσύνης» (Trust Triangle) της Αυτοκυρίαρχης Ταυτότητας (SSI) και η αλληλεπίδραση μεταξύ Εκδότη, Κατόχου και Επαληθευτή.

8.4.1 Τεχνικά Πρότυπα W3C: DIDs και VCs: Η τεχνολογική βάση της SSI έχει τυποποιηθεί από τον οργανισμό World Wide Web Consortium (W3C).

Α. Αποκεντρωμένα Αναγνωριστικά (Decentralized Identifiers - DIDs) Ένα DID είναι ένα μοναδικό αλφαριθμητικό string που λειτουργεί ως παγκόσμια ταυτότητα.

- Μορφή: did:method:specific-idstring (π.χ. did:ethr:0x4f3...).
- Καινοτομία: Σε αντίθεση με το name@gmail.com που ανήκει στην Google, το DID δημιουργείται και ελέγχεται πλήρως από τον χρήστη μέσω ενός ζεύγους κρυπτογραφικών κλειδιών (Public/Private Key). Κανείς δεν μπορεί να το "κατασχέσει".
- DID Document: Κάθε DID συνδέεται με ένα έγγραφο JSON που περιέχει τα δημόσια κλειδιά και τα σημεία εξυπηρέτησης (service endpoints), επιτρέποντας την επαλήθευση χωρίς κεντρικό μητρώο.

Β. Επαληθεύσιμα Διαπιστευτήρια (Verifiable Credentials - VCs) Το DID είναι η "ταυτότητα", αλλά τα VCs είναι τα "προσόντα". Λειτουργούν με το μοντέλο του Τριγώνου Εμπιστοσύνης (Trust Triangle):

1. Εκδότης (Issuer): Η αρχή που πιστοποιεί (π.χ. ένα Πανεπιστήμιο). Υπογράφει ψηφιακά ένα ισχυρισμό (Claim), π.χ. "Ο κάτοχος του DID τάδε έχει πτυχίο Πληροφορικής".
2. Κάτοχος (Holder): Ο φοιτητής, που αποθηκεύει το VC στο ψηφιακό του πορτοφόλι (π.χ. MetaMask, Polygon ID Wallet).
3. Επαληθευτής (Verifier): Ο εργοδότης. Ζητά από τον Κάτοχο απόδειξη πτυχίου.
    - Η Μαγεία: Ο Επαληθευτής ελέγχει την ψηφιακή υπογραφή του Πανεπιστημίου στο Blockchain. Δεν χρειάζεται να επικοινωνήσει με το Πανεπιστήμιο (το οποίο μπορεί να έχει κλείσει). Η εγκυρότητα του πτυχίου είναι μαθηματικά εξασφαλισμένη και αιώνια.

8.4.2 Zero-Knowledge Identity (zk-KYC): Το μεγαλύτερο πρόβλημα με την ταυτότητα είναι η ιδιωτικότητα. Γιατί να δείξω ολόκληρη την ταυτότητά μου (με διεύθυνση, ημερομηνία γέννησης) στον πορτιέρη ενός club, όταν χρειάζεται απλώς να ξέρει ότι είμαι άνω των 18; Η τεχνολογία Zero-Knowledge Proofs (ZKPs) επιτρέπει την Επιλεκτική Αποκάλυψη (Selective Disclosure).

- Το Σενάριο: Ο χρήστης έχει ένα VC ταυτότητας στο πορτοφόλι του.
- Η Απόδειξη: Το πορτοφόλι παράγει μια κρυπτογραφική απόδειξη (ZK-Proof) ότι *"Η ημερομηνία γέννησης στο έγκυρο VC είναι < 2006"*.
- Το Αποτέλεσμα: Ο ελεγκτής λαμβάνει ένα True/False. Δεν βλέπει ποτέ την ημερομηνία, ούτε το όνομα του χρήστη. Πλατφόρμες όπως το Polygon ID (βασισμένο στο πρωτόκολλο Iden3) χρησιμοποιούν Merkle Trees και zk-SNARKs για να υλοποιήσουν αυτό το όραμα, επιτρέποντας ανώνυμη συμμόρφωση (Anonymous Compliance) στο DeFi [69].

8.4.3 Βιομετρία και "Proof of Personhood" (Worldcoin): Στην εποχή της Τεχνητής Νοημοσύνης (AI), το να αποδείξεις ότι είσαι άνθρωπος και όχι Bot είναι κρίσιμο. Το project Worldcoin (συνιδρυτής ο Sam Altman της OpenAI) προτείνει μια ριζοσπαστική λύση:

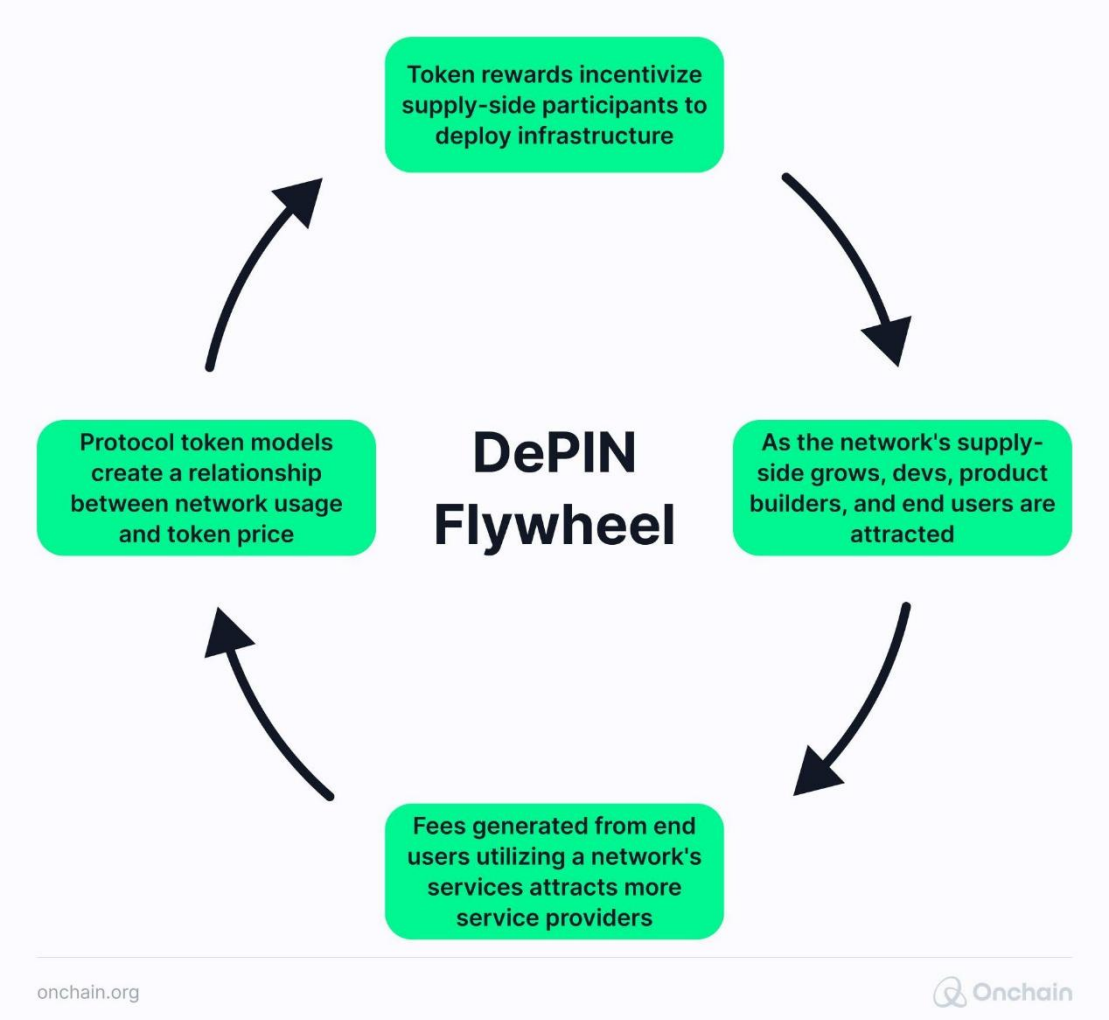
- The Orb: Μια σφαιρική συσκευή σαρώνει την ίριδα του ματιού του χρήστη.
- IrisHash: Η εικόνα της ίριδας μετατρέπεται σε έναν μοναδικό κρυπτογραφικό κωδικό (hash) και η εικόνα διαγράφεται (θεωρητικά).
- World ID: Ο χρήστης λαμβάνει μια ψηφιακή ταυτότητα που αποδεικνύει ότι είναι "μοναδικός άνθρωπος", χωρίς να αποκαλύπτει ποιος είναι.
- Κριτική: Το σύστημα έχει δεχθεί έντονη κριτική για ζητήματα δυστοπικής παρακολούθησης και ασφάλειας των βιομετρικών δεδομένων, οδηγώντας σε απαγορεύσεις σε χώρες όπως η Ισπανία και η Κένυα [70].

8.4.4 Soulbound Tokens (SBT) και Κοινωνική Πίστωση: Τα NFTs (ERC-721) είναι μεταβιβάσιμα. Μπορώ να αγοράσω ένα πτυχίο Harvard ως NFT. Αυτό τα καθιστά ακατάλληλα για ταυτότητα. Ο Vitalik Buterin πρότεινε τα Soulbound Tokens (SBT) στο paper *"Decentralized Society: Finding Web3's Soul"*.

- Ορισμός: Tokens που είναι μόνιμα δεμένα στο πορτοφόλι ("Soul") και δεν μπορούν να μεταφερθούν ή να πωληθούν.
- Χρήσεις:
    1. Ακαδημαϊκά Προσόντα: Πανεπιστημιακά πτυχία που "ζουν" στο Blockchain.
    2. Ιατρικοί Φάκελοι: Ιστορικό ασθενούς που του ανήκει, όχι στο νοσοκομείο.
    3. Under-collateralized Lending: Σήμερα στο DeFi, για να δανειστείς πρέπει να βάλεις ενέχυρο 150%. Με τα SBTs, ένας χρήστης μπορεί να χτίσει "πιστοληπτική φήμη" (Credit Score on-chain) αποπληρώνοντας δάνεια. Πρωτόκολλα μπορούν να του δανείσουν με χαμηλότερο ενέχυρο, βασισμένα στο ιστορικό του, όπως οι τράπεζες [57].

8.5 Αποκεντρωμένα Δίκτυα Φυσικών Υποδομών (DePIN)

Το DePIN (Decentralized Physical Infrastructure Networks) αποτελεί την εφαρμογή της τεχνολογίας Blockchain στη διαχείριση και ανάπτυξη φυσικών υποδομών στον πραγματικό κόσμο. Στόχος είναι η δημιουργία δικτύων (τηλεπικοινωνιών, ενέργειας, αποθήκευσης, αισθητήρων) που χτίζονται και συντηρούνται από τους χρήστες (Crowdsourcing), χωρίς την ανάγκη για κεντρικούς παρόχους όπως η Amazon (AWS) ή η Vodafone. Σύμφωνα με την έκθεση της Messari (2023), το DePIN αξιοποιεί τα κρυπτο-οικονομικά κίνητρα για να μειώσει το κόστος ανάπτυξης υποδομών (Capex) κατά 70-90% σε σύγκριση με τα παραδοσιακά μοντέλα [58].



Εικόνα 8.3: Ο κυκλικός μηχανισμός κινήτρων (Flywheel effect) για την ανάπτυξη των Αποκεντρωμένων Δικτύων Φυσικών Υποδομών (DePIN).

8.5.1 Ταξινομία DePIN: PRNs vs DRNs: Η βιομηχανία διακρίνει τα δίκτυα DePIN σε δύο βασικές κατηγορίες, ανάλογα με τη φύση των πόρων που διαμοιράζονται:

Α. Δίκτυα Φυσικών Πόρων (Physical Resource Networks - PRNs) Απαιτούν την εγκατάσταση υλικού (hardware) σε συγκεκριμένη γεωγραφική τοποθεσία. Η αξία του δικτύου εξαρτάται από την τοποθεσία.

- Παράδειγμα: Το Helium Network (LoRaWAN/5G). Οι χρήστες αγοράζουν Hotspots και τα τοποθετούν στα παράθυρά τους για να παρέχουν σήμα σε IoT συσκευές. Η τοποθεσία είναι κρίσιμη: δέκα hotspots στο ίδιο δωμάτιο είναι άχρηστα, αλλά δέκα σε διαφορετικά τετράγωνα δημιουργούν δίκτυο.
- Αισθητήρες: Το Hivemapper χρησιμοποιεί κάμερες αυτοκινήτου (Dashcams) για να χαρτογραφεί δρόμους σε πραγματικό χρόνο, ανταγωνιζόμενο το Google Street View με κλάσμα του κόστους.

Β. Δίκτυα Ψηφιακών Πόρων (Digital Resource Networks - DRNs) Αφορούν πόρους που είναι ανταλλάξιμοι (fungible) και δεν εξαρτώνται από την τοποθεσία.

- Παράδειγμα: Το Render Network ή το io.net. Ένας χρήστης στην Αθήνα μπορεί να νοικιάσει την κάρτα γραφικών του (GPU) σε έναν ερευνητή AI στη Νέα Υόρκη. Η φυσική θέση της GPU δεν έχει σημασία, αρκεί να έχει γρήγορο Internet.
- Αποθήκευση: Το Filecoin επιτρέπει την ενοικίαση σκληρών δίσκων για αποκεντρωμένο Cloud Storage.

8.5.2 Ο Οικονομικός Κύκλος (The DePIN Flywheel): Το κλασικό πρόβλημα των υποδομών είναι το "Πρόβλημα της Κότας και του Αυγού": Δεν υπάρχουν χρήστες γιατί δεν υπάρχει δίκτυο, και δεν επενδύονται κεφάλαια για δίκτυο γιατί δεν υπάρχουν χρήστες. Το DePIN λύνει αυτό το αδιέξοδο μέσω του Token Incentivization:

1. Bootstrapping: Το πρωτόκολλο εκδίδει tokens και αμείβει τους πρώτους χρήστες (Supply Side) που εγκαθιστούν εξοπλισμό, ακόμα κι αν δεν υπάρχει ακόμα ζήτηση.
2. Growth: Καθώς η κάλυψη αυξάνεται, το δίκτυο γίνεται αξιόπιστο.
3. Demand: Επιχειρήσεις και ιδιώτες αρχίζουν να χρησιμοποιούν το δίκτυο πληρώνοντας τέλη (σε Fiat ή Stablecoins), τα οποία είναι φθηνότερα από τους κεντρικούς παρόχους.
4. Value Capture: Τα έσοδα χρησιμοποιούνται για την αγορά και καταστροφή (Burn) του token του πρωτοκόλλου.
5. Price Appreciation: Η μείωση της προσφοράς tokens αυξάνει την τιμή τους, προσελκύοντας ακόμα περισσότερους παρόχους εξοπλισμού.

8.5.3 Μηχανισμοί Συναίνεσης: Proof of Physical Work (PoPW): Πώς διασφαλίζει το Blockchain ότι ο χρήστης όντως παρέχει την υπηρεσία και δεν τρέχει έναν εξομοιωτή (spoofing) για να κλέψει tokens; Εδώ απαιτούνται εξειδικευμένοι αλγόριθμοι.

Α. Proof of Coverage (PoC) Χρησιμοποιείται στα ασύρματα δίκτυα (π.χ. Helium).

- Beacon: Ένα Hotspot εκπέμπει τυχαία ένα κρυπτογραφημένο σήμα.
- Witnesses: Τα γειτονικά Hotspots που "ακούνε" το σήμα, υπογράφουν κρυπτογραφικά την λήψη του και αναφέρουν την ισχύ του σήματος (RSSI/SNR) στο Blockchain.
- Triangulation: Ο αλγόριθμος χρησιμοποιεί τα δεδομένα των μαρτύρων για να επαληθεύσει τη γεωγραφική θέση του πομπού. Αν τα δεδομένα δεν βγάζουν νόημα (φυσικά αδύνατη απόσταση), ο χρήστης τιμωρείται (slashed).

Β. Proof of Compute (Zero-Knowledge Verifiable Computing) Χρησιμοποιείται στα δίκτυα GPU (π.χ. Render, Akash) για εργασίες AI.

- Πρόβλημα: Πώς ξέρει ο πελάτης ότι η GPU έκανε σωστά τον πολύπλοκο υπολογισμό;
- Λύση: Χρήση τεχνικών όπως το zkML (Zero-Knowledge Machine Learning). Η GPU παράγει όχι μόνο το αποτέλεσμα, αλλά και μια σύντομη κρυπτογραφική απόδειξη ότι το αποτέλεσμα προέκυψε από τη σωστή εκτέλεση του μοντέλου. Αυτό επιτρέπει την επαλήθευση χωρίς να χρειάζεται να ξανατρέξει ο υπολογισμός.

8.5.4 Off-Chain Data Processing και Oracles: Τα δεδομένα που παράγουν τα φυσικά δίκτυα είναι τεράστια (Big Data) και δεν μπορούν να αποθηκευτούν στο Blockchain (θα ήταν πολύ ακριβό). Γι' αυτό, τα DePIN χρησιμοποιούν μια Off-Chain αρχιτεκτονική:

1. Devices: Οι συσκευές υπογράφουν τα δεδομένα (π.χ. συντεταγμένες GPS, θερμοκρασία).
2. Oracle Network: Ένα δίκτυο από κόμβους (Oracles) συγκεντρώνει τα δεδομένα, τα φιλτράρει και τα συμπιέζει.
3. On-Chain Settlement: Μόνο τα αποτελέσματα (π.χ. "Ο χρήστης Α παρείχε 10GB δεδομένων") και οι πληρωμές καταγράφονται στο Blockchain (συνήθως σε φθηνά δίκτυα όπως το Solana ή Layer 2s).

8.5.5 Περιπτώσεις Χρήσης και Αντίκτυπος:

- Τηλεπικοινωνίες: Το Helium Mobile προσφέρει πρόγραμμα κινητής τηλεφωνίας 5G στις ΗΠΑ με $20/μήνα, χρησιμοποιώντας έναν υβριδικό συνδυασμό κεραιών χρηστών και περιαγωγής (roaming) σε μεγάλα δίκτυα (T-Mobile).
- Ενέργεια: Πλατφόρμες όπως το Powerledger επιτρέπουν το Peer-to-Peer Energy Trading. Ένας χρήστης με φωτοβολταϊκά μπορεί να πουλήσει την πλεονάζουσα ενέργεια απευθείας στον γείτονά του μέσω Smart Contract, παρακάμπτοντας τον κεντρικό διαχειριστή και βελτιστοποιώντας την τοπική κατανάλωση.
- Αποθήκευση Δεδομένων: Το Filecoin διαθέτει χωρητικότητα Exabytes, προσφέροντας μια ανθεκτική στη λογοκρισία εναλλακτική στο AWS S3, ιδανική για την αποθήκευση ιστορικών αρχείων και NFTs.

ΚΕΦΑΛΑΙΟ 9: ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΜΕΛΛΟΝΤΙΚΕΣ ΤΑΣΕΙΣ

9.1 Σύνοψη Ευρημάτων: Η Ωρίμανση της Τεχνολογίας και η Νέα Ψηφιακή Υποδομή

Η παρούσα εργασία εξερεύνησε διεξοδικά την τεχνολογική στοίβα (tech stack) που υποστηρίζει την ανάπτυξη των κρυπτονομισμάτων και των κατανεμημένων εφαρμογών. Ξεκινώντας από τους κρυπτογραφικούς αλγορίθμους και φτάνοντας μέχρι τα σύγχρονα δίκτυα φυσικών υποδομών (DePIN), η έρευνα οδηγεί στο αδιαμφισβήτητο συμπέρασμα ότι η τεχνολογία Blockchain δεν αποτελεί πλέον ένα πειραματικό πεδίο για "geeks" ή κερδοσκόπους. Αντιθέτως, έχει εξελιχθεί σε μια στιβαρή, παγκόσμια υποδομή διακανονισμού αξίας (Global Settlement Layer), ικανή να υποστηρίξει την επόμενη γενιά του διαδικτύου και της οικονομίας.

Η ανάλυση των τεχνολογικών δεδομένων οδηγεί σε τέσσερα (4) κεντρικά συμπεράσματα, τα οποία επαναπροσδιορίζουν τον τρόπο που αντιλαμβανόμαστε την ψηφιακή εμπιστοσύνη:

Συμπέρασμα 1: Η Μετάβαση στη Βιωσιμότητα και η "Πράσινη" Συναίνεση

Το πρώτο και ίσως πιο κρίσιμο εύρημα αφορά την περιβαλλοντική εξέλιξη των μηχανισμών συναίνεσης. Όπως αναλύθηκε στο Κεφάλαιο 5, η τεχνολογία ξεκίνησε με το Proof-of-Work (PoW) του Bitcoin, το οποίο, αν και εξαιρετικά ασφαλές, επέβαλε ένα απαγορευτικό ενεργειακό κόστος, καθιστώντας το Blockchain στόχο περιβαλλοντικής κριτικής (ESG concerns).

Η έρευνα έδειξε ότι η βιομηχανία απάντησε αποτελεσματικά σε αυτή την πρόκληση μέσω της μετάβασης στο Proof-of-Stake (PoS), με κορυφαίο παράδειγμα το "The Merge" του Ethereum το 2022. Τα δεδομένα αποδεικνύουν ότι:

- Η κατανάλωση ενέργειας μειώθηκε κατά 99.95%, μετατρέποντας το Blockchain από ενεργειακό "μαύρο πρόβατο" σε μια τεχνολογία φιλικότερη προς το περιβάλλον ακόμα και από το παραδοσιακό τραπεζικό σύστημα (το οποίο απαιτεί φυσικά καταστήματα και servers).
- Η ασφάλεια του δικτύου δεν μειώθηκε, αλλά άλλαξε μορφή: από "φυσική" (Hardware/Electricity) έγινε "οικονομική" (Staking/Slashing).
- Αυτό το βήμα ήταν απαραίτητο για τη θεσμική υιοθέτηση, καθώς επέτρεψε σε εταιρείες με αυστηρά κριτήρια ESG (όπως η BlackRock και η Visa) να χτίσουν πάνω στο Ethereum χωρίς ρίσκο φήμης.

Συμπέρασμα 2: Η Αρχιτεκτονική Λύση στο Τρίλημμα της Επεκτασιμότητας

Το δεύτερο συμπέρασμα ανατρέπει την παλαιότερη αντίληψη ότι "τα blockchains είναι αργά και ακριβά". Όπως αναλύθηκε στο Κεφάλαιο 7, το Τρίλημμα της Επεκτασιμότητας (η αδυναμία ταυτόχρονης επίτευξης Ασφάλειας, Αποκέντρωσης και Ταχύτητας) δεν λύθηκε σε ένα επίπεδο, αλλά παρακάμφθηκε μέσω της Αρθρωτής Αρχιτεκτονικής (Modular Architecture).

Η μελέτη των Layer 2 λύσεων (Rollups) και των τεχνολογιών Data Availability (DA) δείχνει ότι:

- Διαχωρίσαμε τις λειτουργίες: Το Ethereum (Layer 1) παρέχει πλέον μόνο την Ασφάλεια και τον Διακανονισμό, ενώ τα Rollups (Layer 2) αναλαμβάνουν την Εκτέλεση.
- Η εισαγωγή των Blobs (EIP-4844) και των Zero-Knowledge Proofs επέτρεψε τη μείωση του κόστους συναλλαγής από $5-$10 σε λιγότερο από $0.01, καθιστώντας βιώσιμες τις μικρο-συναλλαγές και τις κοινωνικές εφαρμογές.
- Πλέον, η τεχνολογία μπορεί να υποστηρίξει χιλιάδες συναλλαγές το δευτερόλεπτο (TPS), πλησιάζοντας τις επιδόσεις των κεντρικοποιημένων συστημάτων (Visa/Mastercard), διατηρώντας όμως την εγγύηση της αποκέντρωσης.

Συμπέρασμα 3: Από την Κερδοσκοπία στην Πραγματική Οικονομία (RWA & Tokenization)

Το τρίτο και πιο σημαντικό οικονομικό συμπέρασμα, όπως προέκυψε από το Κεφάλαιο 8, είναι ότι το Blockchain παύει να είναι αυτο-αναφορικό (κρυπτονομίσματα που αγοράζονται για να αγοραστούν άλλα κρυπτονομίσματα) και συνδέεται με την πραγματική οικονομία. Η Τοκενοποίηση Πραγματικών Περιουσιακών Στοιχείων (RWA) αποτελεί το "Killer App" της δεκαετίας.

Η ανάλυση των προτύπων ERC-3643 και των θεσμικών κινήσεων έδειξε ότι:

- Η τεχνολογία προσφέρει άμεση εκκαθάριση (T+0 settlement) έναντι του παραδοσιακού T+2, απελευθερώνοντας τρισεκατομμύρια δολάρια δεσμευμένων κεφαλαίων.
- Η δυνατότητα προγραμματισμού του χρήματος (Programmable Money) μέσω έξυπνων συμβολαίων επιτρέπει αυτοματοποιημένες διαδικασίες (π.χ. αυτόματη πληρωμή μερισμάτων, συμμόρφωση KYC σε πραγματικό χρόνο) που ήταν αδύνατες με τα παλιά συστήματα βάσεων δεδομένων.
- Η είσοδος παραδοσιακών κολοσσών (TradFi) στον χώρο, μέσω tokenized ομολόγων και ETFs, επιβεβαιώνει ότι το Blockchain θα αποτελέσει το "back-end" του μελλοντικού χρηματοπιστωτικού συστήματος.

Συμπέρασμα 4: Η Επανάσταση της Ψηφιακής Κυριαρχίας και Ιδιωτικότητας

Τέλος, η έρευνα ανέδειξε μια θεμελιώδη αλλαγή στο μοντέλο διαχείρισης ταυτότητας και δεδομένων. Σε έναν κόσμο που κυριαρχείται από την Τεχνητή Νοημοσύνη (AI) και τα Deepfakes, η ικανότητα απόδειξης της "ανθρωπότητας" και της προέλευσης των δεδομένων γίνεται υπαρξιακή ανάγκη.

Η μελέτη της Αυτοκυρίαρχης Ταυτότητας (SSI) και των Zero-Knowledge Proofs (ZKPs) στο Κεφάλαιο 8 κατέδειξε ότι:

- Μεταβαίνουμε από το μοντέλο της "Φεουδαρχικής Ταυτότητας" (όπου η Google/Facebook κατέχουν τα δεδομένα μας) στο μοντέλο της "Κυρίαρχης Ταυτότητας" (όπου ο χρήστης ελέγχει τα διαπιστευτήριά του μέσω κρυπτογραφίας).
- Η τεχνολογία ZKPs επιτρέπει για πρώτη φορά στην ιστορία την απόδειξη μιας ιδιότητας χωρίς την αποκάλυψη της πληροφορίας (π.χ. απόδειξη ενηλικίωσης χωρίς επίδειξη ημερομηνίας γέννησης). Αυτό λύνει το αιώνιο πρόβλημα της σύγκρουσης μεταξύ διαφάνειας (Public Blockchain) και ιδιωτικότητας (GDPR).
- Τα ρυθμιστικά πλαίσια όπως το MiCA στην Ευρώπη δεν "σκοτώνουν" την τεχνολογία, αλλά την νομιμοποιούν, θέτοντας τους κανόνες για την ασφαλή μετάβαση στο Web3.

Συνοψίζοντας, η παρούσα διατριβή καταλήγει στο ότι οι τεχνολογίες που αναλύθηκαν δεν αποτελούν απλώς μια βελτίωση των υφιστάμενων συστημάτων πληρωμών, αλλά μια αλλαγή παραδείγματος (paradigm shift). Περνάμε από το "Internet of Information", όπου αντιγράφουμε αρχεία, στο "Internet of Value", όπου μεταφέρουμε μοναδική αξία, με μαθηματική βεβαιότητα, χωρίς μεσάζοντες και με απόλυτη διαφάνεια.

9.2 Η Κβαντική Απειλή και η Μετάβαση στη Μετα-Κβαντική Κρυπτογραφία (Post-Quantum Cryptography - PQC)

Η ασφάλεια του Bitcoin, του Ethereum και του παγκόσμιου τραπεζικού συστήματος στηρίζεται σε μια θεμελιώδη υπόθεση: ότι ορισμένα μαθηματικά προβλήματα είναι τόσο δύσκολα, που ακόμα και ο ισχυρότερος υπερυπολογιστής θα χρειαζόταν δισεκατομμύρια χρόνια για να τα λύσει. Η έλευση των Κβαντικών Υπολογιστών (Quantum Computers) απειλεί να καταρρίψει αυτή την υπόθεση, οδηγώντας μας στο λεγόμενο "Y2Q" (Year to Quantum) — το χρονικό σημείο όπου η κλασική κρυπτογραφία θα καταστεί άχρηστη.

9.2.1 Η Μαθηματική Ευπάθεια: Ο Αλγόριθμος του Shor: Οι σημερινοί αλγόριθμοι ασύμμετρης κρυπτογραφίας (Public Key Cryptography), όπως ο RSA και η Ελλειπτική Κρυπτογραφία (ECC - secp256k1) που χρησιμοποιεί το Bitcoin, βασίζονται στη δυσκολία της παραγοντοποίησης μεγάλων αριθμών ή του προβλήματος του διακριτού λογάριθμου.

- Το Πρόβλημα: Ένας κλασικός υπολογιστής λειτουργεί με bits (0 ή 1). Για να βρει το ιδιωτικό κλειδί από το δημόσιο, πρέπει να κάνει δοκιμές σειριακά (Brute Force), κάτι πρακτικά αδύνατο.
- Η Κβαντική Λύση: Ένας κβαντικός υπολογιστής χρησιμοποιεί Qubits, τα οποία λόγω της αρχής της *Υπέρθεσης (Superposition)*, μπορούν να βρίσκονται σε κατάσταση 0 και 1 ταυτόχρονα.
- Shor’s Algorithm: Ο Peter Shor απέδειξε το 1994 ότι ένας κβαντικός υπολογιστής με επαρκή αριθμό qubits μπορεί να λύσει το πρόβλημα του διακριτού λογάριθμου σε πολυωνυμικό χρόνο. Αυτό σημαίνει ότι θα μπορούσε να παραγάγει το Ιδιωτικό Κλειδί

(Private Key) οποιουδήποτε πορτοφολιού, γνωρίζοντας μόνο το Δημόσιο Κλειδί (Public Key).

9.2.2 Το Σενάριο Επίθεσης στο Blockchain: Πώς ακριβώς θα γινόταν μια επίθεση; Σύμφωνα με τους Aggarwal et al. (2021), υπάρχουν δύο διανύσματα επίθεσης:

Α. Επίθεση σε "Παλιές" Διευθύνσεις (P2PK) Στα πρώτα χρόνια του Bitcoin (Pay-to-Public-Key), το Δημόσιο Κλειδί ήταν ορατό στο blockchain. Τα νομίσματα του Satoshi Nakamoto (~1 εκατ. BTC) βρίσκονται σε τέτοιες διευθύνσεις. Ένας κβαντικός υπολογιστής θα μπορούσε να υπολογίσει τα ιδιωτικά κλειδιά και να κλέψει αυτά τα νομίσματα, προκαλώντας κατάρρευση της αγοράς.

Β. Επίθεση κατά τη διάρκεια της Συναλλαγής Στις σύγχρονες διευθύνσεις (P2PKH), το Δημόσιο Κλειδί αποκαλύπτεται μόνο *όταν* ο χρήστης ξοδεύει τα χρήματα.

- Ο χρήστης στέλνει μια συναλλαγή.
- Η συναλλαγή μπαίνει στο Mempool και το Δημόσιο Κλειδί αποκαλύπτεται.
- Ο κβαντικός επιτιθέμενος βλέπει τη συναλλαγή, υπολογίζει αστραπιαία το Ιδιωτικό Κλειδί και στέλνει μια δική του συναλλαγή με υψηλότερο fee (Front-running) για να μεταφέρει τα χρήματα στον εαυτό του *πριν* η αρχική συναλλαγή μπει σε μπλοκ. Αυτό απαιτεί έναν κβαντικό υπολογιστή εξαιρετικά γρήγορο (να σπάει το κλειδί σε <10 λεπτά).

9.2.3 Ανθεκτικότητα των Hash Functions (Grover's Algorithm): Σε αντίθεση με τις ψηφιακές υπογραφές, οι συναρτήσεις κατακερματισμού (SHA-256, Keccak-256) είναι πιο ανθεκτικές. Ο κβαντικός αλγόριθμος του Grover επιταχύνει την εύρεση αντιστρόφου hash, αλλά μόνο τετραγωνικά (όχι εκθετικά).

- Πρακτικά: Αυτό σημαίνει ότι το SHA-256 γίνεται τόσο ασφαλές όσο το SHA-128. Η λύση είναι απλή: απλά διπλασιάζουμε το μήκος των hashes (π.χ. SHA-512) και είμαστε ασφαλείς. Γι' αυτό οι διευθύνσεις που δεν έχουν χρησιμοποιηθεί ποτέ (και άρα δεν έχουν αποκαλύψει το Public Key τους) θεωρούνται "Quantum Safe" [80].

9.2.4 Λύσεις: Μετα-Κβαντική Κρυπτογραφία (PQC): Η επιστημονική κοινότητα, υπό την καθοδήγηση του NIST (National Institute of Standards and Technology), έχει ήδη αναπτύξει αλγόριθμους που αντέχουν σε κβαντικές επιθέσεις.

Α. Κρυπτογραφία Πλέγματος (Lattice-based Cryptography) Οι αλγόριθμοι αυτοί (π.χ. CRYSTALS-Kyber και Dilithium) βασίζονται σε προβλήματα γεωμετρίας πλέγματος πολλών διαστάσεων. Ακόμα και ένας κβαντικός υπολογιστής δεν μπορεί να βρει το "κοντινότερο διάνυσμα" (Shortest Vector Problem) σε ένα πλέγμα 500 διαστάσεων αποδοτικά. Αυτοί οι αλγόριθμοι θα αντικαταστήσουν το ECDSA.

Β. ZK-STARKs (Hash-based Proofs) Τα Zero-Knowledge STARKs (σε αντίθεση με τα SNARKs) βασίζονται αποκλειστικά σε Hash functions και όχι σε ελλειπτικές καμπύλες. Επομένως, θεωρούνται εγγενώς Quantum Resistant. Τα δίκτυα που χρησιμοποιούν STARKs (όπως το StarkNet) είναι ήδη έτοιμα για την κβαντική εποχή.

9.2.5 Στρατηγική Μετάβασης και Κρυπτογραφική Ευελιξία: Το μεγαλύτερο πρόβλημα δεν είναι η εύρεση του νέου αλγορίθμου, αλλά η αναβάθμιση του συστήματος. Πώς αλλάζουμε την κλειδαριά σε ένα σπίτι (Bitcoin) ενώ κατοικείται, χωρίς να πετάξουμε έξω τους ενοίκους;

1. Soft/Hard Forks: Τα δίκτυα θα πρέπει να εισάγουν νέους τύπους διευθύνσεων (PQC Addresses). Οι χρήστες θα πρέπει να μεταφέρουν τα κεφάλαιά τους από τις παλιές διευθύνσεις στις νέες.
2. Account Abstraction (ERC-4337): Στο Ethereum, η "Αφαίρεση Λογαριασμού" επιτρέπει τον διαχωρισμό της λογικής επικύρωσης από το πρωτόκολλο. Ένα έξυπνο συμβόλαιο-πορτοφόλι μπορεί να προγραμματιστεί ώστε να δέχεται υπογραφές Lamport ή Winternitz (που είναι quantum safe) αντί για ECDSA, χωρίς να χρειαστεί αναβάθμιση όλου του Ethereum. Αυτή η ιδιότητα ονομάζεται Cryptographic Agility (Κρυπτογραφική Ευελιξία).

9.3 Η Σύγκλιση AI και Blockchain: Η Οικονομία των Αυτόνομων Πρακτόρων (The Agentic Economy)

Ενώ η Τεχνητή Νοημοσύνη (GenAI) παρέχει στις μηχανές τη δυνατότητα να σκέφτονται και να δημιουργούν, το Blockchain τους παρέχει τη δυνατότητα να κατέχουν αξία και να συναλλάσσονται. Ο Vitalik Buterin (2024) περιγράφει αυτή τη σχέση ως εξής: *"Η AI είναι ο εγκέφαλος, το Blockchain είναι το σώμα (εκτέλεση) και τα κρυπτονομίσματα είναι το αίμα (ρευστότητα)"*. Αυτή η ένωση οδηγεί στη δημιουργία της Machine-to-Machine (M2M) Economy, όπου αυτόνομοι πράκτορες λογισμικού (AI Agents) εκτελούν πολύπλοκες οικονομικές εργασίες χωρίς ανθρώπινη παρέμβαση.

9.3.1 Το Πρόβλημα των Τραπεζών και η Λύση του Web3: Ένα AI Agent (π.χ. ένας προσωπικός βοηθός που κλείνει αεροπορικά εισιτήρια) δεν μπορεί να ανοίξει τραπεζικό λογαριασμό. Οι τράπεζες απαιτούν φυσική παρουσία, ταυτότητα και υπογραφή (KYC), πράγματα που ένα λογισμικό δεν διαθέτει.

- Η Λύση: Τα πορτοφόλια κρυπτονομισμάτων είναι Permissionless. Ένα AI μπορεί να δημιουργήσει μια διεύθυνση Ethereum σε χιλιοστά του δευτερολέπτου, να λάβει USDC και να πληρώσει για υπηρεσίες (π.χ. API access, server hosting) αυτόματα.
- Account Abstraction (ERC-4337): Αυτό το πρότυπο επιτρέπει στα AI Agents να προγραμματίζουν τις πληρωμές τους (π.χ. "Πλήρωσε μόνο αν η πτήση δεν ακυρωθεί") και να ανακτούν πρόσβαση αν "ξεχάσουν" το κλειδί τους, καθιστώντας τα πλήρως αυτόνομα οικονομικά υποκείμενα [83].

9.3.2 Zero-Knowledge Machine Learning (zkML): Καθώς τα μοντέλα AI (όπως το GPT-4) λαμβάνουν αποφάσεις για τη ζωή μας (π.χ. έγκριση δανείου, ιατρική διάγνωση), προκύπτει το πρόβλημα του "Μαύρου Κουτιού": *Πώς ξέρουμε ότι το μοντέλο έτρεξε σωστά και δεν αλλοιώθηκε το αποτέλεσμα για να μας αδικήσει;* Το Blockchain δεν μπορεί να τρέξει AI (είναι πολύ αργό). Η λύση είναι το zkML.

- Λειτουργία: Το μοντέλο AI τρέχει εκτός αλυσίδας (Off-chain) σε ισχυρές GPUs.

- Η Απόδειξη: Μαζί με το αποτέλεσμα, το σύστημα παράγει μια κρυπτογραφική απόδειξη (ZK-Proof) ότι *"Το αποτέλεσμα Χ παρήχθη από το Μοντέλο Υ με τα Δεδομένα Ζ"*.
- Επαλήθευση: Το έξυπνο συμβόλαιο στο Blockchain ελέγχει την απόδειξη (που είναι μικρή και φθηνή). Αν είναι έγκυρη, εκτελεί την πληρωμή/απόφαση. Αυτό επιτρέπει τη δημιουργία Αποκεντρωμένων Hedge Funds, όπου μια AI διαχειρίζεται κεφάλαια και αποδεικνύει στους επενδυτές ότι ακολουθεί τη στρατηγική που υποσχέθηκε, χωρίς να αποκαλύψει τον μυστικό της αλγόριθμο (Model Weight Privacy) [84].

9.3.3 Ακεραιότητα Περιεχομένου (Content Authenticity) ενάντια στα Deepfakes:

Στην εποχή της Generative AI, η διάκριση μεταξύ πραγματικού και ψεύτικου βίντεο είναι σχεδόν αδύνατη. Τα Deepfakes απειλούν τη δημοκρατία και την οικονομία. Το Blockchain προσφέρει τη λύση μέσω της Κρυπτογραφικής Υπογραφής Προέλευσης.

- C2PA Standard & Blockchain: Κάμερες και κινητά τηλέφωνα θα ενσωματώνουν τσιπ που υπογράφουν ψηφιακά κάθε φωτογραφία τη στιγμή της λήψης (hashing).
- Immutability: Το hash της φωτογραφίας εγγράφεται στο Blockchain.
- Verification: Όταν ένας χρήστης βλέπει μια είδηση, ο browser ελέγχει αν το hash της εικόνας ταιριάζει με αυτό στο Blockchain. Αν ταιριάζει, η εικόνα είναι αυθεντική. Αν όχι, έχει παραποιηθεί από AI. Πρωτόκολλα όπως το Numbers Protocol ή το Starling Lab χρησιμοποιούνται ήδη για την τεκμηρίωση εγκλημάτων πολέμου, ώστε να μην μπορούν να αμφισβητηθούν ως "fake news".

9.3.4 Αποκεντρωμένη Εκπαίδευση (DePIN for AI Training): Η ανάπτυξη της AI ελέγχεται σήμερα από ελάχιστες εταιρείες (OpenAI, Google, Anthropic) επειδή μόνο αυτές έχουν πρόσβαση σε χιλιάδες κάρτες γραφικών (GPUs). Το Blockchain εκδημοκρατίζει την πρόσβαση μέσω δικτύων DePIN (όπως αναλύθηκε στο 8.5, π.χ. Gensyn, Bittensor).

- Gensyn Protocol: Επιτρέπει την εκπαίδευση ενός μοντέλου AI σε χιλιάδες μικρούς υπολογιστές ταυτόχρονα. Το Blockchain επαληθεύει ότι κάθε μικρός υπολογιστής έκανε σωστά τη δουλειά του (μέσω Probabilistic Proofs) και τον πληρώνει.
- Bittensor (TAO): Δημιουργεί μια "αγορά νοημοσύνης". Διαφορετικά μοντέλα AI ανταγωνίζονται για να δώσουν την καλύτερη απάντηση σε ένα ερώτημα. Οι άλλοι κόμβοι αξιολογούν την απάντηση και το Blockchain επιβραβεύει το εξυπνότερο μοντέλο. Αυτό δημιουργεί μια συλλογική νοημοσύνη (Hive Mind) που δεν ελέγχεται από κανέναν CEO.

9.3.5 Μοντέλα ως NFTs (IP-NFTs): Στο μέλλον, τα ίδια τα μοντέλα AI ή τα datasets θα είναι tokenized.

- Data Ownership: Σήμερα, η AI εκπαιδεύεται στα δεδομένα μας δωρεάν. Στο Web3, οι χρήστες θα κατέχουν τα δεδομένα τους ως NFTs. Αν μια εταιρεία θέλει να εκπαιδεύσει την AI της στα ιατρικά μου δεδομένα, θα πρέπει να πληρώσει το "Data NFT" μου μέσω έξυπνου συμβολαίου.
- Royalty Distribution: Κάθε φορά που το AI μοντέλο παράγει κέρδος, ένα ποσοστό θα πηγαίνει αυτόματα στους δημιουργούς των δεδομένων εκπαίδευσης.

9.4 Το Μέλλον της Χρηστικότητας: Αφαίρεση Λογαριασμού και Αρχιτεκτονική Προθέσεων (Abstraction & Intents)

Για να φτάσει το Blockchain στο επόμενο δισεκατομμύριο χρηστών, πρέπει να πάψει να μοιάζει με το MS-DOS και να αρχίσει να μοιάζει με το iOS. Η τρέχουσα πολυπλοκότητα (διαχείριση ιδιωτικών κλειδιών, υπολογισμός Gas fees, επιλογή δικτύου) αποτελεί το μεγαλύτερο εμπόδιο υιοθέτησης. Η λύση έρχεται μέσα από δύο επαναστατικές τεχνολογίες: την Αφαίρεση Λογαριασμού (Account Abstraction) και τα Intents.

9.4.1 Αφαίρεση Λογαριασμού (Account Abstraction - ERC-4337): Μέχρι σήμερα, οι λογαριασμοί στο Ethereum (EOA - Externally Owned Accounts) ήταν "χαζοί": απλώς ένα ζεύγος κλειδιών. Αν χάσεις το κλειδί, χάνεις τα πάντα. Το πρότυπο ERC-4337 μετατρέπει κάθε πορτοφόλι σε Έξυπνο Συμβόλαιο (Smart Account). Αυτό επιτρέπει:

- Social Recovery: Ξέχασες τον κωδικό σου; Δεν πειράζει. Μπορείς να ανακτήσεις πρόσβαση αν 3 από τους 5 φίλους σου ("Guardians") επιβεβαιώσουν την ταυτότητά σου, ή μέσω του Google λογαριασμού σου. Τέλος στο άγχος της "Seed Phrase".
- Gas Abstraction (Paymaster): Ο χρήστης δεν χρειάζεται να έχει ETH για να πληρώσει τα τέλη συναλλαγής. Μπορεί να πληρώσει με USDC (Stablecoin) ή η εφαρμογή να επιδοτήσει τα τέλη (Sponsored Transactions) για να προσελκύσει πελάτες, όπως ακριβώς το Web2 (δεν πληρώνουμε server costs για να μπούμε στο Facebook).
- Batching: Πολλαπλές ενέργειες (π.χ. Έγκριση + Ανταλλαγή + Κατάθεση) γίνονται με ένα κλικ και μία υπογραφή, αντί για τρεις.

9.4.2 Αρχιτεκτονική Προθέσεων (Intent-Centric Architecture): Η σημερινή αλληλεπίδραση με το Blockchain είναι "Προστακτική" (Imperative): Ο χρήστης πρέπει να πει στο σύστημα *πώς* ακριβώς να εκτελέσει μια ενέργεια (βήμα-βήμα). Το μέλλον είναι "Δηλωτικό" (Declarative), βασισμένο σε Intents.

- Τι είναι το Intent: Ο χρήστης δεν υπογράφει μια συναλλαγή ("στείλε 1 ETH στο 0x..."). Υπογράφει μια Πρόθεση ("Θέλω να έχω 1000 USDC στο Arbitrum με το ελάχιστο δυνατό κόστος").
- Solvers: Ένα δίκτυο από εξειδικευμένους αλγόριθμους (Solvers/Fillers) ανταγωνίζεται για το ποιος θα εκπληρώσει την επιθυμία του χρήστη πιο γρήγορα και φθηνά. Ο χρήστης δεν ενδιαφέρεται αν τα χρήματα πήγαν μέσω Uniswap ή Curve, ή ποια γέφυρα χρησιμοποιήθηκε.
- Αποτέλεσμα: Ο χρήστης ορίζει το Τι (Επιθυμητό Αποτέλεσμα) και οι Solvers αναλαμβάνουν το Πώς (Διαδρομή Εκτέλεσης). Αυτό αφαιρεί όλη την τεχνική πολυπλοκότητα από τον τελικό χρήστη [87].

9.4.3 Αφαίρεση Αλυσίδας (Chain Abstraction): Σε ένα μέλλον με χιλιάδες Rollups (Optimism, Base, Zora), ο κατακερματισμός της ρευστότητας είναι πρόβλημα. Ο χρήστης δεν πρέπει να ξέρει σε ποια αλυσίδα βρίσκεται. Η Αφαίρεση Αλυσίδας (που προωθείται από δίκτυα όπως το NEAR και το Polygon AggLayer) δημιουργεί την ψευδαίσθηση μιας ενιαίας αλυσίδας.

- Ο χρήστης έχει ένα υπόλοιπο (π.χ. $50).
- Όταν αγοράζει ένα NFT στο δίκτυο Base, το σύστημα αυτόματα γεφυρώνει τα χρήματα από το Optimism στο παρασκήνιο (σε milliseconds), χωρίς ο χρήστης να καταλάβει ότι άλλαξε δίκτυο.
- Αυτό οδηγεί στην εμπειρία του "Superchain": Ένα ενιαίο, διασυνδεδεμένο δίκτυο εφαρμογών.

9.4.4 Συμπέρασμα Ενότητας: Η τεχνολογία γίνεται πραγματικά επαναστατική όταν γίνεται αόρατη. Με την Αφαίρεση Λογαριασμού και τα Intents, το Blockchain μετατρέπεται από ένα δύσχρηστο εργαλείο για ειδικούς σε μια αόρατη υποδομή (backend) που τροφοδοτεί εφαρμογές τις οποίες μπορεί να χρησιμοποιήσει ο καθένας, χωρίς να γνωρίζει καν ότι χρησιμοποιεί Blockchain.

9.5 Θεσμική Υιοθέτηση και το Όραμα του "Finternet": Ένα Ενιαίο Παγκόσμιο Καθολικό

Το 2024 θα μείνει στην ιστορία ως το έτος που το Blockchain έπαψε να είναι "εναλλακτικό" και έγινε "θεσμικό". Η έγκριση των Spot Bitcoin και Ethereum ETFs στις ΗΠΑ, σε συνδυασμό με το ρυθμιστικό πλαίσιο MiCA στην Ευρώπη, σηματοδότησε το τέλος της φάσης των "Early Adopters". Πλέον, βρισκόμαστε στη φάση της Θεσμικής Ενσωμάτωσης (Institutional Integration), όπου οι μεγαλύτεροι διαχειριστές κεφαλαίων στον κόσμο (BlackRock, Fidelity, Franklin Templeton) δεν επενδύουν απλώς σε κρυπτονομίσματα, αλλά χτίζουν τις υποδομές τους πάνω σε αυτά.

9.5.1 Το Ορόσημο των ETFs και η Νομιμοποίηση της Κατηγορίας Περιουσιακών Στοιχείων:

Η έγκριση των Spot ETFs από την Επιτροπή Κεφαλαιαγοράς των ΗΠΑ (SEC) άλλαξε θεμελιωδώς τη δομή της αγοράς.

- Το Πρόβλημα πριν τα ETFs: Τα συνταξιοδοτικά ταμεία (Pension Funds) και οι σύμβουλοι επενδύσεων δεν μπορούσαν νομικά να αγοράσουν Bitcoin, καθώς απαιτούσε πολύπλοκη θεματοφυλακή (Custody) και λογιστική διαχείριση που δεν υποστήριζαν τα παραδοσιακά συστήματα.
- Η Λύση: Το ETF μετατρέπει το Bitcoin σε έναν τίτλο που διαπραγματεύεται στο χρηματιστήριο (όπως η μετοχή της Apple). Αυτό "ξεκλείδωσε" τρισεκατομμύρια δολάρια αδρανούς κεφαλαίου.
- Η Σημασία: Η κίνηση αυτή αναγνώρισε de facto το Bitcoin ως "Ψηφιακό Χρυσό" (Store of Value) και το Ethereum ως "Ψηφιακό Πετρέλαιο" (Tech Commodity), εντάσσοντάς τα στα χαρτοφυλάκια 60/40 των παραδοσιακών επενδυτών.

9.5.2 Το Όραμα του "Finternet" και το Ενιαίο Καθολικό (Unified Ledger): Τον Απρίλιο του 2024, η Τράπεζα Διεθνών Διακανονισμών (BIS) - η "Κεντρική Τράπεζα των Κεντρικών Τραπεζών" - δημοσίευσε ένα ιστορικό έγγραφο οραματιζόμενη το "Finternet": ένα χρηματοπιστωτικό σύστημα για το μέλλον. Σύμφωνα με τους Carstens et al. (2024), το σημερινό σύστημα είναι αργό γιατί το χρήμα και τα περιουσιακά στοιχεία ζουν σε ξεχωριστές βάσεις δεδομένων (Silos). Για να αγοράσεις μια μετοχή, πρέπει να κινηθούν χρήματα από την τράπεζα Α στην τράπεζα Β, και τίτλοι από το αποθετήριο C στο αποθετήριο D. Αυτός ο συγχρονισμός παίρνει μέρες (T+2).

Η BIS προτείνει το Unified Ledger (Ενιαίο Καθολικό): Μια κοινή ψηφιακή υποδομή όπου συνυπάρχουν:

1. Χρήμα Κεντρικής Τράπεζας (Wholesale CBDC): Για την τελική εκκαθάριση.
2. Τοκενοποιημένες Καταθέσεις (Tokenized Deposits): Χρήμα εμπορικών τραπεζών.
3. Τοκενοποιημένα Περιουσιακά Στοιχεία (Tokenized Assets): Μετοχές, ομόλογα, ακίνητα.

Σε αυτό το περιβάλλον, όλες οι συναλλαγές είναι Ατομικές (Atomic): Η μεταβίβαση του τίτλου και η πληρωμή γίνονται ταυτόχρονα στο ίδιο μπλοκ. Αν δεν περάσει η πληρωμή, δεν μεταβιβάζεται ο τίτλος. Ο κίνδυνος αθέτησης (counterparty risk) εξαλείφεται πλήρως.

9.5.3 Από το T+2 στο T+0: Η Επανάσταση της Εκκαθάρισης: Το παραδοσιακό σύστημα διακανονισμού (Settlement) βασίζεται σε κεντρικούς διαμεσολαβητές όπως το DTCC στις ΗΠΑ ή το Euroclear στην Ευρώπη.

- Το Κόστος της Καθυστέρησης: Το γεγονός ότι χρειάζονται 2 ημέρες (T+2) για να εκκαθαριστεί μια πώληση μετοχής σημαίνει ότι δισεκατομμύρια δολάρια παραμένουν "δεσμευμένα" ως εγγύηση (collateral) για να καλυφθεί ο κίνδυνος ότι κάποιο μέρος θα χρεοκοπήσει στο ενδιάμεσο.
- Η Λύση του Blockchain: Με την τοκενοποίηση, η εκκαθάριση γίνεται Instant (T+0). Ο Larry Fink, CEO της BlackRock, δήλωσε χαρακτηριστικά: *"Η τοκενοποίηση είναι η επόμενη γενιά για τις αγορές. Θα έχουμε στιγμιαίο διακανονισμό και μειωμένα τέλη. Αλλά το πιο σημαντικό είναι ότι θα έχουμε εξατομικευμένες στρατηγικές μέσω έξυπνων συμβολαίων"*. Το λανσάρισμα του BlackRock USD Institutional Digital Liquidity Fund (BUIDL) στο Ethereum το 2024 ήταν η πρώτη έμπρακτη εφαρμογή αυτού του οράματος: ένα αμοιβαίο κεφάλαιο που ζει στο Blockchain και προσφέρει ρευστότητα 24/7/365.

9.5.4 Stablecoins: Το Νέο Σύστημα Πληρωμών: Ενώ τα CBDCs είναι ακόμα στη φάση του σχεδιασμού, τα Stablecoins (ιδίως USDT και USDC) έχουν ήδη γίνει το de facto μέσο διασυνοριακών πληρωμών, αντικαθιστώντας σταδιακά το σύστημα SWIFT σε αναδυόμενες αγορές.

- Όγκος Συναλλαγών: Το 2024, ο όγκος διακανονισμού των Stablecoins ξεπέρασε αυτόν της Visa.
- Χρήση: Εταιρείες όπως η Stripe και η PayPal ενσωμάτωσαν τα Stablecoins για πληρωμές, επιτρέποντας σε έναν προγραμματιστή στη Νιγηρία να πληρωθεί από μια εταιρεία στις ΗΠΑ σε δευτερόλεπτα, με ελάχιστο κόστος, παρακάμπτοντας το αργό τραπεζικό σύστημα.

- Προγραμματιζόμενες Πληρωμές: Τα Stablecoins επιτρέπουν σύνθετες ροές χρήματος, όπως το Streaming Money (π.χ. πληρωμή μισθού ανά δευτερόλεπτο εργασίας) μέσω πρωτοκόλλων όπως το Sablier, κάτι αδύνατο με το παραδοσιακό τραπεζικό σύστημα.

9.5.5 Η Νέα Χρηματοοικονομική Στοίβα (The New Financial Stack): Συνοψίζοντας, οδεύουμε προς μια πλήρη αντικατάσταση της παγκόσμιας χρηματοοικονομικής υποδομής ("The Plumbing").

- Παλιά Στοίβα: SWIFT (Μηνύματα) -> Τράπεζες (Λογιστικά βιβλία) -> Κεντρικές Τράπεζες (Εκκαθάριση) -> CSDs (Τίτλοι). Πολλά διαφορετικά βιβλία που πρέπει να συμφωνηθούν (Reconciliation).
- Νέα Στοίβα: Blockchain (Κοινό Καθολικό) -> Smart Contracts (Λογική Συναλλαγών) -> Tokens (Περιουσιακά Στοιχεία & Χρήμα). Όλοι βλέπουν την ίδια αλήθεια σε πραγματικό χρόνο.

9.6 Τελικό Συμπέρασμα: Η Μετάβαση στο Διαδίκτυο της Αξίας (The Internet of Value)

Η παρούσα πτυχιακή εργασία ξεκίνησε με την εξέταση μιας τεχνολογίας που γεννήθηκε μέσα στις φλόγες της παγκόσμιας χρηματοπιστωτικής κρίσης του 2008. Το Bitcoin του Satoshi Nakamoto ήταν αρχικά μια πράξη διαμαρτυρίας ενάντια στη διάβρωση της εμπιστοσύνης στο τραπεζικό σύστημα. Δεκαπέντε χρόνια αργότερα, η τεχνολογία αυτή έχει εξελιχθεί από ένα περιθωριακό πείραμα σε μια παγκόσμια υποδομή θεσμικής εμπιστοσύνης.

Μέσα από την ανάλυση των οκτώ προηγούμενων κεφαλαίων, καταλήγουμε σε ένα θεμελιώδες συμπέρασμα: Δεν βιώνουμε απλώς την ψηφιοποίηση του χρήματος, αλλά την αναδιάταξη της αρχιτεκτονικής του διαδικτύου και της οικονομίας.

9.6.1 Η Αλλαγή Παραδείγματος: Από την Πληροφορία στην Αξία: Το διαδίκτυο, όπως το γνωρίζαμε μέχρι σήμερα (Web2), ήταν το "Internet of Information". Ήταν σχεδιασμένο για την αντιγραφή και τη διάδοση δεδομένων. Όταν στέλνω ένα email ή ένα PDF, δεν στέλνω το πρωτότυπο· στέλνω ένα αντίγραφο και κρατάω το πρωτότυπο. Αυτό είναι ιδανικό για την πληροφορία, αλλά καταστροφικό για την αξία (χρήμα, τίτλοι ιδιοκτησίας), όπου το "διπλό ξόδεμα" (double-spending) πρέπει να αποφευχθεί πάση θυσία. Το Blockchain λύνει αυτό το πρόβλημα εισάγοντας την Ψηφιακή Σπανιότητα (Digital Scarcity). Για πρώτη φορά στην ιστορία, μπορούμε να μεταφέρουμε ένα ψηφιακό αντικείμενο σε κάποιον άλλον και να είμαστε μαθηματικά βέβαιοι ότι δεν το έχουμε πλέον εμείς. Αυτό επιτρέπει τη δημιουργία του "Internet of Value": Ένα παγκόσμιο δίκτυο όπου η αξία μετακινείται τόσο εύκολα, γρήγορα και φθηνά όσο η πληροφορία σήμερα.

9.6.2 Η Μηχανική της Εμπιστοσύνης (Trust Engineering): Η κοινωνία μας λειτουργεί βασιζόμενη σε ενδιάμεσους εμπιστοσύνης (Trusted Third Parties): Τράπεζες, Συμβολαιογράφους,

Κυβερνήσεις, Big Tech εταιρείες. Τους πληρώνουμε "ενοίκιο" (rents) για να διασφαλίζουν ότι οι συναλλαγές μας είναι έγκυρες. Το Blockchain αντικαθιστά τη θεσμική εμπιστοσύνη με την Κρυπτογραφική Αλήθεια (Cryptographic Truth).

- Δεν εμπιστευόμαστε ότι η τράπεζα έχει τα χρήματά μας· το επαληθεύουμε στο καθολικό (Proof of Reserves).
- Δεν εμπιστευόμαστε ότι η εταιρεία θα τηρήσει τη συμφωνία· εμπιστευόμαστε το Έξυπνο Συμβόλαιο (Code is Law). Αυτή η μετάβαση από το *"Don't be evil"* (το μότο της Google) στο *"Can't be evil"* (η υπόσχεση του Bitcoin) μειώνει δραστικά το κόστος της εμπιστοσύνης και εξαλείφει τη διαφθορά και την αυθαιρεσία των μεσαζόντων.

9.6.3 Η Σύγκλιση Τεχνολογιών (The Convergence): Η πραγματική δύναμη του Blockchain αποκαλύπτεται όταν συνδυάζεται με τις άλλες εκθετικές τεχνολογίες του 21ου αιώνα:

1. Με την Τεχνητή Νοημοσύνη (AI): Το Blockchain δίνει στην AI οικονομική αυτονομία και διαφάνεια (zkML), αποτρέποντας τη δημιουργία "μαύρων κουτιών".
2. Με το IoT (DePIN): Το Blockchain επιτρέπει στις μηχανές να συναλλάσσονται μεταξύ τους, δημιουργώντας μια αυτόνομη Machine Economy.
3. Με την Κβαντική Υπολογιστική: Η προσαρμογή σε μετα-κβαντικούς αλγορίθμους θα θωρακίσει την ψηφιακή οικονομία για τον επόμενο αιώνα.

9.6.4 Κοινωνικός Αντίκτυπος: Συμπερίληψη και Κυριαρχία: Πέρα από την τεχνολογία, ο αντίκτυπος είναι βαθιά ανθρωπιστικός.

- Χρηματοοικονομική Συμπερίληψη: 1,7 δισεκατομμύρια άνθρωποι δεν έχουν πρόσβαση σε τράπεζες (Unbanked). Το Blockchain τους δίνει πρόσβαση στην παγκόσμια οικονομία μόνο με ένα κινητό τηλέφωνο.
- Ιδιοκτησία Δεδομένων: Μέσω της Αυτοκυρίαρχης Ταυτότητας (SSI), οι χρήστες ανακτούν τον έλεγχο της ψηφιακής τους ζωής από τις πλατφόρμες.
- Διαφάνεια: Οι δημόσιες δαπάνες και οι φιλανθρωπίες μπορούν να παρακολουθούνται σε πραγματικό χρόνο, μειώνοντας τη σπατάλη και την απάτη.

9.6.5 Επίλογος: Το Τέλος της Αρχής Βρισκόμαστε στο τέλος της "εποχής της ανακάλυψης" και στην αρχή της "εποχής της εφαρμογής". Τα κρυπτονομίσματα δεν είναι πλέον μια κερδοσκοπική φούσκα, αλλά τα θεμέλια ενός νέου χρηματοπιστωτικού συστήματος (Finternet). Όπως το πρωτόκολλο TCP/IP έγινε αόρατο αλλά πανταχού παρόν, έτσι και το Blockchain θα γίνει η αόρατη υποδομή που τρέχει στο παρασκήνιο της παγκόσμιας οικονομίας. Οι προκλήσεις που απομένουν —ρυθμιστικές, ενεργειακές, κβαντικές— είναι υπαρκτές, αλλά οι λύσεις τους έχουν ήδη δρομολογηθεί. Το ερώτημα δεν είναι πλέον *αν* το Blockchain θα επιτύχει, αλλά *πόσο γρήγορα* θα μετασχηματίσει τον κόσμο μας.

Η επανάσταση δεν θα μεταδοθεί τηλεοπτικά· θα επικυρωθεί στο επόμενο μπλοκ.

ΠΙΝΑΚΑΣ ΟΡΟΛΟΓΙΑΣ (GLOSSARY)

Αλγόριθμος Κατακερματισμού — Hashing Algorithm
Αλυσίδα Συστοιχιών (Μπλοκ) — Blockchain
Αμετάβλητο — Immutability
Ανεκτικότητα σε Βυζαντινά Σφάλματα — Byzantine Fault Tolerance (BFT)
Ανθεκτικότητα στη Λογοκρισία — Censorship Resistance
Ανταλλακτήριο — Exchange (CEX / DEX)
Απόδειξη Εργασίας — Proof of Work (PoW)
Απόδειξη Μηδενικής Γνώσης — Zero-Knowledge Proof (ZKP)
Απόδειξη Συμμετοχής (ή Δέσμευσης) — Proof of Stake (PoS)
Αποκεντρωμένη Εφαρμογή — Decentralized Application (DApp)
Αποκεντρωμένη Χρηματοδότηση — Decentralized Finance (DeFi)
Αποκεντρωμένος Αυτόνομος Οργανισμός — Decentralized Autonomous Organization (DAO)
Αποκεντρωμένα Δίκτυα Φυσικών Υποδομών — Decentralized Physical Infrastructure Networks (DePIN)
Αρθρωτή Αρχιτεκτονική — Modular Architecture
Αυτοκυρίαρχη Ταυτότητα — Self-Sovereign Identity (SSI)
Γέφυρα (Διασύνδεση Αλυσίδων) — Bridge (Cross-chain Bridge)
Δέντρο Merkle — Merkle Tree
Δημόσιο / Ιδιωτικό Κλειδί — Public / Private Key
Διακλάδωση (Σκληρή / Ήπια) — Fork (Hard / Soft)
Δίκτυο Ομότιμων Κόμβων — Peer-to-Peer (P2P) Network
Διπλή Δαπάνη — Double Spending
Εικονική Μηχανή Ethereum — Ethereum Virtual Machine (EVM)
Έξυπνο Συμβόλαιο — Smart Contract
Εξόρυξη — Mining
Επικεφαλίδα Μπλοκ — Block Header
Επιφάνεια Επίθεσης — Attack Surface
Κατανεμημένο Καθολικό — Distributed Ledger Technology (DLT)
Κόμβος — Node
Κρυπτογραφία Ελλειπτικών Καμπυλών — Elliptic Curve Cryptography (ECC)
Λύσεις Δευτέρου Επιπέδου — Layer 2 Solutions
Μετα-Κβαντική Κρυπτογραφία — Post-Quantum Cryptography (PQC)
Μηχανισμός Συναίνεσης — Consensus Mechanism
Μη-Ανταλλάξιμο Διακριτικό — Non-Fungible Token (NFT)
Μονάδα Κόστους Εκτέλεσης (Καύσιμο) — Gas (Ethereum)
Μοντέλο Μη-Δαπανηθέντων Εξόδων — Unspent Transaction Output (UTXO)
Πορτοφόλι — Wallet
Πραγματικά Περιουσιακά Στοιχεία — Real World Assets (RWA)
Σπόρος Ανάκτησης (Φράση) — Seed Phrase / Mnemonic Phrase
Συναθροίσεις — Rollups (Optimistic & ZK)
Συνάρτηση Σύνοψης (Hash) — Hash Function
Τεχνολογία Κατανεμημένου Καθολικού — Distributed Ledger Technology (DLT)

Τοκενοποίηση (ή Διακριτοποίηση) — Tokenization
Υπερπληθωρισμός — Hyperinflation
Φίλτρο Bloom — Bloom Filter
Χρησμός (Πάροχος Δεδομένων) — Oracle
Ψηφιακό Νόμισμα Κεντρικής Τράπεζας — Central Bank Digital Currency (CBDC)
Ψηφιακή Υπογραφή — Digital Signature

ΠΙΝΑΚΑΣ ΣΥΝΤΜΗΣΕΩΝ & ΑΚΡΩΝΥΜΙΩΝ

AI: Artificial Intelligence
AML: Anti-Money Laundering
ASIC: Application-Specific Integrated Circuit
BFT: Byzantine Fault Tolerance
CAP: Consistency, Availability, Partition Tolerance
CBDC: Central Bank Digital Currency
DAG: Directed Acyclic Graph
DApp: Decentralized Application
DeFi: Decentralized Finance
DePIN: Decentralized Physical Infrastructure Networks
DLT: Distributed Ledger Technology
DPoS: Delegated Proof of Stake
ECC: Elliptic Curve Cryptography
ECDSA: Elliptic Curve Digital Signature Algorithm
ETF: Exchange-Traded Fund
EVM: Ethereum Virtual Machine
FBA: Federated Byzantine Agreement
IoT: Internet of Things KYC: Know Your Customer
MiCA: Markets in Crypto-Assets
NFT: Non-Fungible Token
P2P: Peer-to-Peer
PBFT: Practical Byzantine Fault Tolerance
PoS: Proof of Stake
PoW: Proof of Work
PQC: Post-Quantum Cryptography
RWA: Real World Assets
SEC: Securities and Exchange Commission
SHA: Secure Hash Algorithm
SPV: Simplified Payment Verification
SSI: Self-Sovereign Identity
SWIFT: Society for Worldwide Interbank Financial Telecommunication
TPS: Transactions Per Second
UTXO: Unspent Transaction Output
ZK / ZKP: Zero-Knowledge Proof

ΒΙΒΛΙΟΓΡΑΦΙΑ (REFERENCES)

1. **Hassan, M. U., Rehmani, M. H., & Chen, J. (2019).** Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future directions. *Future Generation Computer Systems*, 97, 512-529.
2. **Casino, F., Dasaklis, T. K., & Patsakis, C. (2019).** A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36, 55-81.
3. **Gai, K., Guo, J., Zhu, L., & Yu, S. (2020).** Blockchain technology in internet of things: A comprehensive survey. *IEEE Internet of Things Journal*, 7(8), 7858-7878.
4. **Wang, Q., Li, R., Wang, Q., & Chen, S. (2021).** Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. *arXiv preprint arXiv:2105.07447*.
5. **Zhou, Q., Huang, H., Zheng, Z., & Bian, J. (2020).** Solutions to scalability of blockchain: A survey. *IEEE Access*, 8, 16453-16466.
6. **Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020).** A survey on the security of blockchain systems. *Future Generation Computer Systems*, 107, 841-853.
7. **Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020).** A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, 22(2), 1432-1465.
8. **Nakamoto, S. (2008).** Bitcoin: A Peer-to-Peer Electronic Cash System. *Whitepaper*. Available at: https://bitcoin.org/bitcoin.pdf
9. **Buterin, V. (2013).** Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. *Whitepaper*. Available at: https://ethereum.org/en/whitepaper/
10. **Wood, G. (2014).** Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014), 1-32.
11. **Antonopoulos, A. M. (2017).** *Mastering Bitcoin: Programming the open blockchain*. O'Reilly Media.
12. **Szabo, N. (1996).** Smart contracts: building blocks for digital markets. *Extropy*, 16(2), 50-62.
13. **Back, A. (2002).** Hashcash - A Denial of Service Counter-Measure.
14. **Chung, M., Kim, J., & Hong, J. W. K. (2021).** UTXO-based vs. account-based: A comparative analysis of blockchain models. *International Journal of Network Management*, 31(2), e2137.
15. **King, S., & Nadal, S. (2012).** PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake.
16. **Wegrzyn, K. E., & Wang, E. (2021).** Types of blockchain: Consensus algorithms and open source blockchain platforms. In *Managing distributed cloud applications and infrastructure* (pp. 1-20). Springer.
17. **Dwork, C., & Naor, M. (1992).** Pricing via processing or combatting junk mail. *Advances in Cryptology—CRYPTO'92*, 139-147.
18. **Lamport, L., Shostak, R., & Pease, M. (1982).** The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems*, 4(3), 382-401.
19. **Castro, M., & Liskov, B. (1999).** Practical Byzantine Fault Tolerance. *OSDI*, 99, 173-186.
20. **Eyal, I., & Sirer, E. G. (2014).** Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM*, 61(7), 95-102.
21. **Garay, J., Kiayias, A., & Leonardos, N. (2015).** The bitcoin backbone protocol: Analysis and applications. *Annual International Conference on the Theory and Applications of Cryptographic Techniques*.

22. **Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014).** Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake. *SIGMETRICS Performance Evaluation Review*.
23. **Gilad, Y., Hemo, R., Micali, S., Vlachos, G., & Zeldovich, N. (2017).** Algorand: Scaling byzantine agreements for cryptocurrencies. *Proceedings of the 26th Symposium on Operating Systems Principles*.
24. **Kwon, J. (2014).** Tendermint: Consensus without Mining. *Whitepaper*.
25. **Diffie, W., & Hellman, M. (1976).** New directions in cryptography. *IEEE transactions on Information Theory*, 22(6), 644-654.
26. **Rivest, R. L., Shamir, A., & Adleman, L. (1978).** A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120-126.
27. **Merkle, R. C. (1987).** A digital signature based on a conventional encryption function. *Advances in Cryptology—CRYPTO'87*.
28. **Koblitz, N. (1987).** Elliptic curve cryptosystems. *Mathematics of computation*, 48(177), 203-209.
29. **Zarir, A. A., Oliva, G. A., Jiang, Z. M., & Hassan, A. E. (2021).** Developing cost-effective blockchain applications. *IEEE Software*, 38(3), 50-55.
30. **Werner, S. M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., & Knottenbelt, W. J. (2021).** SoK: Decentralized finance (DeFi). *arXiv preprint arXiv:2101.08769*.
31. **Beniiche, A. (2020).** A study of blockchain oracles. *arXiv preprint arXiv:2004.07140*.
32. **Qin, K., Zhou, L., & Gervais, A. (2021).** Quantifying blockchain extractable value: How dark is the forest? *2021 IEEE Symposium on Security and Privacy (SP)*, 198-214.
33. **Chen, W., Xu, Z., Shi, S., Zhao, Y., & Zhao, J. (2020).** A survey of blockchain-based identity management models. *IEEE Access*, 8, 35003-35028.
34. **Feist, J., Griego, G., & Ross, S. (2021).** Crytic.io: ERC-4626 Tokenized Vault Standard. *Ethereum Improvement Proposals, no. 4626*.
35. **Loesch, S., Hindman, N., Richardson, M. B., & Welch, N. (2021).** Impermanent loss in uniswap v3. *arXiv preprint arXiv:2111.09192*.
36. **Gudgeon, L., Perez, D., Harz, D., Livshits, B., & Knottenbelt, W. J. (2020).** The decentralized financial crisis: Attacking DeFi protocols via flash loans. *arXiv preprint arXiv:2002.08099*.
37. **Breidenbach, L., Cahill, C., Carter, B., Coventry, A., Juels, A., & Nazarov, S. (2021).** Chainlink 2.0: Next steps in the evolution of decentralized oracle networks. *Chainlink Whitepaper*.
38. **Caldarelli, G. (2020).** Understanding the blockchain oracle problem: A call for action. *Information*, 11(11), 509.
39. **Sayeed, S., Marco-Gisbert, H., & Caira, T. (2020).** Smart contract vulnerabilities: A systematic review. *IEEE Access*, 8, 114532-114550.
40. **Perez, D., & Livshits, B. (2021).** Smart contract vulnerabilities: Vulnerability sources and security patterns. *arXiv preprint arXiv:1908.08605*.
41. **Tolmach, P., Li, Y., Lin, S. W., Liu, Y., & Li, Z. (2021).** A survey of smart contract formal verification tools. *ACM Computing Surveys (CSUR)*, 54(7), 1-38.
42. **Wu, K., Ma, Y., Huang, G., & Liu, X. (2021).** A first look at blockchain-based decentralized finance (DeFi) oracles. *Proceedings of the 2021 IEEE International Conference on Blockchain*.
43. **Schar, F. (2021).** Decentralized Finance: On Blockchain-and Smart Contract-Based Financial Markets. *Federal Reserve Bank of St. Louis Review*, 103(2), 153-174.
44. **Zhou, Q., Huang, H., Zheng, Z., & Bian, J. (2020).** Solutions to scalability of blockchain: A survey. *IEEE Access*, 8, 16453-16466.

45. **Hafid, A., Hafid, A. S., & Samih, M. (2020).** Scaling blockchains: A comprehensive survey. *IEEE Access*, 8, 125244-125262.
46. **Belchior, R., Vasconcelos, A., Guerreiro, S., & Correia, M. (2021).** A survey on blockchain interoperability: Past, present, and future trends. *ACM Computing Surveys (CSUR)*, 54(8), 1-41.
47. **Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P., & Gervais, A. (2020).** SoK: Layer-two blockchain protocols. *International Conference on Financial Cryptography and Data Security*.
48. **Li, R., Qi, H., & Wang, Q. (2020).** Sidechains and cross-chain technology: A survey. *IEEE Access*, 8, 125244-125262.
49. **Adler, J., Al-Bassam, M., & Sonnino, A. (2022).** Celestia: A scalable general-purpose data availability layer. *Celestia Whitepaper*.
50. **Buterin, V., et al. (2022).** EIP-4844: Shard Blob Transactions. *Ethereum Improvement Proposals*.
51. **Chainlink Labs. (2023).** Chainlink Cross-Chain Interoperability Protocol (CCIP) Whitepaper.
52. **Zamyatin, A., Al-Bassam, M., Zindros, D., Kokoris-Kogias, E., Moreno-Sanchez, P., ... & McCorry, P. (2021).** SoK: Communication across distributed ledgers. *International Conference on Financial Cryptography and Data Security*.
53. **Xie, T., Zhang, J., Zerick, & Song, D. (2022).** zkBridge: Trustless cross-chain bridges made practical. *ACM CCS 2022*.
54. **Citigroup. (2023).** Money, Tokens, and Games: Blockchain's Next Billion Users and Trillions in Value. *Citi GPS: Global Perspectives & Solutions*.
55. **Bank for International Settlements (BIS). (2023).** Making headway - Results of the 2022 BIS survey on central bank digital currencies and crypto. *BIS Papers No 136*.
56. **European Parliament. (2023).** Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA). *Official Journal of the European Union*.
57. **Buterin, V., Weyl, E. G., & Ohlhaver, P. (2022).** Decentralized society: Finding web3's soul. *Available at SSRN*.
58. **Messari. (2023).** State of DePIN 2023. *Messari Research*.
59. **Goldman Sachs. (2023).** Digital Assets: From Hype to Reality. *Investment Research*.
60. **Chainlink Labs. (2023).** Chainlink Proof of Reserve: Transparency for Real-World Assets. *Whitepaper*.
61. **Centrifuge. (2022).** Real World Assets: Bridging DeFi and Traditional Finance. *Centrifuge Protocol Documentation*.
62. **OECD. (2023).** The Tokenisation of Assets and Potential Implications for Financial Markets. *OECD Blockchain Policy Series*.
63. **Zetzsche, D. A., Annunziata, F., Arner, D. W., & Ross, R. P. (2021).** The markets in crypto-assets regulation (MiCA) and the EU digital finance strategy. *Capital Markets Law Journal*, 16(2), 203-225.
64. **Maume, P. (2021).** Philipp Maume on the European Commission's Proposal for a Regulation on Markets in Crypto-Assets (MiCA). *Available at SSRN*.
65. **Federal Reserve Bank of Boston & MIT Digital Currency Initiative. (2022).** Project Hamilton Phase 1 Executive Summary. *Technical Report*.
66. **Bank for International Settlements (BIS). (2022).** Project Tourbillon: Auditable privacy for CBDCs. *BIS Innovation Hub Swiss Centre*.
67. **Auer, R., Cornelli, G., & Frost, J. (2020).** Rise of the central bank digital currencies: Drivers, approaches and technologies. *BIS Working Papers No 880*.

68. **European Central Bank (ECB). (2023).** Report on the investigation phase of the digital euro. *ECB Publications*.
69. **Polygon Labs. (2023).** Polygon ID: Identity Infrastructure for Web3. *Whitepaper*.
70. **Worldcoin Foundation. (2023).** A Technical Explanation of the Worldcoin Protocol. *Whitepaper*.
71. **W3C. (2022).** Decentralized Identifiers (DIDs) v1.0. *W3C Recommendation*.
72. **Ballandies, M. C., et al. (2023).** A taxonomy of decentralized physical infrastructure networks. *arXiv preprint arXiv:2305.XXXX*.
73. **Helium Foundation. (2022).** Proof-of-Coverage: Technical Whitepaper.
74. **Messari. (2024).** State of DePIN 2024: The Year of Adoption. *Messari Research*.
75. **Io.net. (2023).** The Decentralized Compute Network: Architecture and Consensus. *Whitepaper*.
76. **NIST. (2023).** Post-Quantum Cryptography Standardization. *National Institute of Standards and Technology Reports*.
77. **Buterin, V. (2024).** The promise and challenges of Crypto + AI applications. *Vitalik.ca*.
78. **Bank for International Settlements (BIS). (2024).** The Finternet: the financial system for the future. *BIS Working Papers*.
79. **World Economic Forum. (2024).** The Future of Financial Infrastructure. *WEF Insight Report*.
80. **Aggarwal, D., Brennen, G. K., Lee, T., Santha, M., & Tomamichel, M. (2021).** Quantum attacks on Bitcoin, and how to protect against them. *Ledger*, 3.
81. **NIST. (2022).** NIST Announces First Four Quantum-Resistant Cryptographic Algorithms. *NIST News Release*.
82. **Buterin, V. (2021).** STARKs, Part I: Proofs with Polynomials. *Vitalik.ca*.
83. **Modulus Labs. (2023).** The Case for Zero-Knowledge Machine Learning (zkML). *Modulus Research*.
84. **Gensyn. (2022).** A Trustless Deep Learning Compute Protocol. *Litepaper*.
85. **Bittensor. (2023).** Internet of Intelligence: The TAO Whitepaper.
86. **Paradigm. (2023).** Intent-Based Architectures and their Risks. *Paradigm Research*.
87. **Buterin, V., et al. (2021).** ERC-4337: Account Abstraction Using Alt Mempool. *Ethereum Improvement Proposals*.
88. **Near Protocol. (2024).** Chain Abstraction: The Future of Web3 UX. *Near Foundation Whitepaper*.
89. **Carstens, A., et al. (2023).** Blueprint for the future monetary system: improving the old, enabling the new. *BIS Annual Economic Report*.
90. **BlackRock. (2024).** 2024 Annual Letter to Investors: Tokenization. *BlackRock Investor Relations*.
91. **Citi GPS. (2023).** Money, Tokens, and Games: Blockchain's Next Billion Users. *Citigroup Global Perspectives & Solutions*.
92. **Feist, J., & Dankrad, F. (2023).** KZG Polynomial Commitments. *Ethereum Research*.
93. **Tapscott, D., & Tapscott, A. (2016).** *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. Penguin.
94. **Antonopoulos, A. M. (2014).** *The Internet of Money*. Merkle Bloom LLC.
95. **Brewer, E. A. (2000).** Towards robust distributed systems. *Proceedings of the nineteenth annual ACM symposium on Principles of distributed computing*, 7.

96. **Popov, S. (2018).** The Tangle. *IOTA Whitepaper v1.4.3*. Available at: https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf

97. **Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Yellick, K. (2018).** Hyperledger fabric: a distributed operating system for permissioned blockchains. *Proceedings of the thirteenth EuroSys conference*, 1-15.

98. **Wuille, P., et al. (2015).** BIP 141: Segregated Witness (Consensus layer). *Bitcoin Improvement Proposals*. Available at: https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki

99. **Buterin, V. (2015).** On Public and Private Blockchains. *Ethereum Blog*. Available at: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains

100. **Cachin, C., & Vukolić, M. (2017).** Blockchain consensus protocols in the wild. *arXiv preprint arXiv:1707.01873*.