



Πτυχιακή Εργασία

Τίτλος (Ελληνικά)	Τεχνολογίες κρυπτονομισμάτων: Blockchain, εφαρμογές και κοινωνικοοικονομική επίδραση
Τίτλος (Αγγλικά)	Cryptocurrency Technologies: Blockchain, Applications and Socio-economic Impact
Ονοματεπώνυμο Φοιτητή	Ιωάννης Μπαλκούρας
Πατρώνυμο	Ιωάννης
Αριθμός Μητρώου	Π21228
Επιβλέπων	Κωνσταντίνος Λιαγκούρας, Επίκουρος Καθηγητής
Ημερομηνία Παράδοσης	Σεπτέμβριος 2026

Copyright © Ιωάννης Μπαλκούρας, 2026

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν αποκλειστικά τον συγγραφέα και δεν αντιπροσωπεύουν τις επίσημες θέσεις του Πανεπιστημίου Πειραιώς.

Δήλωση περί Λογοκλοπής

Ως συγγραφέας της παρούσας εργασίας δηλώνω πως η παρούσα εργασία δεν αποτελεί προϊόν λογοκλοπής και δεν περιέχει υλικό από μη αναφερόμενες πηγές.

Ευχαριστίες

Στο σημείο αυτό, επιθυμώ να εκφράσω τις θερμές μου ευχαριστίες προς τον επιβλέποντα καθηγητή μου, κ. Κωνσταντίνο Λιαγκούρα, για την εμπιστοσύνη που μου έδειξε αναθέτοντάς μου αυτό το θέμα. Επιπλέον, θα ήθελα να ευχαριστήσω συνολικά το διδακτικό προσωπικό του Τμήματος Πληροφορικής του Πανεπιστημίου Πειραιώς. Η παρούσα εργασία βασίστηκε σημαντικά στα εφόδια και το επιστημονικό υπόβαθρο που αποκόμισα από τα μαθήματα του προγράμματος σπουδών. Οι γνώσεις που μου προσέφεραν οι καθηγητές μου σε τομείς όπως η ασφάλεια πληροφοριακών συστημάτων, η διαχείριση δεδομένων και η αλγοριθμική σκέψη, υπήρξαν θεμελιώδεις για την κατανόηση και την ανάλυση των τεχνολογιών που εξετάζονται στην πτυχιακή μου μελέτη.

Περίληψη

Η παρούσα διπλωματική εργασία πραγματεύεται την τεχνολογία των Κατανεμημένων Καθολικών (Distributed Ledger Technology - DLT) και το οικοσύστημα των κρυπτονομισμάτων, προσεγγίζοντάς τα όχι απλώς ως καινοτόμα χρηματοοικονομικά εργαλεία, αλλά πρωτίστως ως θεμελιώδεις υποδομές της σύγχρονης επιστήμης της πληροφορικής. Ο κύριος σκοπός της μελέτης είναι η εις βάθος τεχνική ανάλυση των μηχανισμών που καθιστούν δυνατή την αποκεντρωμένη μεταφορά αξίας και πληροφορίας σε περιβάλλοντα «μηδενικής εμπιστοσύνης» (trustless environments), καταργώντας πλήρως την ανάγκη ενδιάμεσων κεντρικών καταπιστευμάτων.

Αρχικά, εξετάζεται το δομικό τεχνολογικό υπόβαθρο, δίνοντας έμφαση στην αρχιτεκτονική των δομών δεδομένων (blocks), τον κρίσιμο ρόλο των μονόδρομων κρυπτογραφικών συναρτήσεων κατακερματισμού (hashing), την Ασύμμετρη Κρυπτογραφία Ελλειπτικών Καμπυλών (ECC) και τους αλγορίθμους επίτευξης κατανεμημένης συναίνεσης, όπως η Απόδειξη Εργασίας (Proof of Work) και η Απόδειξη Συμμετοχής (Proof of Stake). Στη συνέχεια, η μελέτη εμβαθύνει στην εξέλιξη του δικτύου από απλά συστήματα διακανονισμού συναλλαγών σε πλήρως προγραμματιζόμενα (Turing-complete) περιβάλλοντα, αναλύοντας την αρχιτεκτονική των Έξυπνων Συμβολαίων (Smart Contracts) και την Τοκενοποίηση Πραγματικών Περιουσιακών Στοιχείων (Real World Assets - RWA).

Στο επίπεδο των εφαρμογών, η έρευνα επικεντρώνεται στην Αποκεντρωμένη Χρηματοοικονομική (DeFi) και τη λειτουργία των Αυτοματοποιημένων Ειδικών Διαπραγματευτών (AMMs), διερευνώντας πώς ο ντετερμινιστικός κώδικας αντικαθιστά τις παραδοσιακές τραπεζικές υπηρεσίες. Παράλληλα, αναλύεται η δυναμική της «Οικονομίας της Προσοχής» (Attention Economy) μέσω της συμπεριφορικής ανάλυσης των memecoins. Η κοινωνικοοικονομική αξιολόγηση αναδεικνύει τις προοπτικές για παγκόσμια χρηματοοικονομική συμπερίληψη, αλλά και τις κρίσιμες προκλήσεις κυβερνοασφάλειας, συμπεριλαμβανομένων των ευπαθειών σε επίπεδο λογισμικού (smart contract exploits, rug pulls) και του τεχνολογικού βάρους της αυτοφύλαξης (self-custody) των ιδιωτικών κλειδιών.

Μέσα από μια συστηματική βιβλιογραφική ανασκόπηση, η εργασία καταλήγει σε μια συγκριτική αξιολόγηση των σύγχρονων αρχιτεκτονικών βάσει του «Τριλήμματος του Blockchain». Τα τελικά συμπεράσματα υποδεικνύουν ότι η μελλοντική βιωσιμότητα, η βιομηχανική κλιμάκωση και η μαζική υιοθέτηση του οικοσυστήματος εξαρτώνται άμεσα από τις λύσεις Δεύτερου Επιπέδου (Layer-2 Rollups), την ενσωμάτωση Αποδείξεων Μηδενικής Γνώσης (ZKPs) για την ιδιωτικότητα, καθώς και την ανάπτυξη ασφαλών πρωτοκόλλων διαλειτουργικότητας (Cross-Chain Bridges / Layer 0) με τα αναδυόμενα ψηφιακά νομίσματα κρατικών φορέων (CBDCs).

Λέξεις Κλειδιά: Blockchain, Κρυπτονομίσματα, Έξυπνα Συμβόλαια, Αποκεντρωμένη Χρηματοοικονομική (DeFi), Κρυπτογραφία, Λύσεις Layer-2, Τοκενοποίηση (RWA), Διαλειτουργικότητα.

Abstract

This thesis investigates Distributed Ledger Technology (DLT) and the cryptocurrency ecosystem, approaching them not merely as innovative financial tools, but primarily as fundamental infrastructures of modern computer science. The main objective of this study is the in-depth technical analysis of the mechanisms that enable the decentralized transfer of value and information in "trustless environments," completely eliminating the need for centralized trusted intermediaries.

Initially, the structural technological background is examined, with an emphasis on the architecture of data structures (blocks), the critical role of one-way cryptographic hash functions, Elliptic Curve Cryptography (ECC), and distributed consensus algorithms, such as Proof of Work and Proof of Stake. Subsequently, the study delves into the network's evolution from simple transaction settlement systems to fully programmable (Turing-complete) environments, analyzing the architecture of Smart Contracts and the Tokenization of Real World Assets (RWA).

At the application level, the research focuses on Decentralized Finance (DeFi) and the operation of Automated Market Makers (AMMs), exploring how deterministic code replaces traditional banking services. Concurrently, the dynamics of the "Attention Economy" are analyzed through the behavioral assessment of memecoins. The socio-economic evaluation highlights the prospects for global financial inclusion, as well as critical cybersecurity challenges, including software vulnerabilities (smart contract exploits, rug pulls) and the technological burden of private key self-custody.

Through a systematic literature review, the thesis concludes with a comparative evaluation of modern architectures based on the "Blockchain Trilemma." The final conclusions indicate that the future sustainability, industrial scaling, and mass adoption of the ecosystem directly depend on Layer-2 solutions (Rollups), the integration of Zero-Knowledge Proofs (ZKPs) for privacy, and the development of secure interoperability protocols (Cross-Chain Bridges / Layer 0) alongside emerging Central Bank Digital Currencies (CBDCs).

Keywords: Blockchain, Cryptocurrencies, Smart Contracts, Decentralized Finance (DeFi), Cryptography, Layer-2 Solutions, Real World Assets (RWA), Interoperability.

Περιεχόμενα

Copyright © Ιωάννης Μπαλκούρας, 2026	1
Ευχαριστίες.....	2
Περίληψη	3
Abstract	4
Περιεχόμενα	5
Κατάλογος Εικόνων.....	8
1.1 Το Πλαίσιο της Αποκεντρωμένης Τεχνολογίας και το Web3.....	9
1.2 Κίνητρο και Σκοπός της Πτυχιακής Εργασίας	10
1.2 Διάρθρωση της Πτυχιακής	10
1.3 Το Πρόβλημα των Βυζαντινών Στρατηγών (Byzantine Generals Problem).....	11
1.3.1 Η Θεωρητική Αλληγορία και ο Ορισμός του Προβλήματος	11
1.3.2 Βυζαντινή Ανοχή Σφαλμάτων (Byzantine Fault Tolerance - BFT)	12
1.3.3 Η Λύση του Satoshi Nakamoto: Proof of Work και Οικονομικά Κίνητρα.....	12
2. Ιστορική Αναδρομή και το Κίνημα των Cypherpunks	13
2.1 Το Κίνημα των Cypherpunks: Η Κρυπτογραφία ως Κοινωνικό Εργαλείο	13
2.2 Οι Πρόδρομοι του Ψηφιακού Χρήματος: Τα Αποτυχημένα (αλλά κρίσιμα) Πειράματα.....	13
2.3 Η Οικονομική Κρίση του 2008 και το Genesis Block.....	13
2.4 Η Εξέλιξη: Από το Απλό Χρήμα στα Προγραμματιζόμενα Συμβόλαια (Smart Contracts).....	14
3. Τεχνολογικό Υπόβαθρο και Βασικές Έννοιες	16
3.1 Τεχνολογία Blockchain: Αρχιτεκτονική και Δομή Blocks	16
3.1.1 Η Κεφαλίδα του Μπλοκ (Block Header)	16
3.1.2 Το Σώμα του Μπλοκ (Block Body)	16
3.1.3 Το Genesis Block και το Φαινόμενο της Χιονοστιβάδας	17
3.2 Κρυπτογραφικές Συναρτήσεις Κατακερματισμού (Hashing) και SHA-256	17
3.3 Μηχανισμοί Συναίνεσης (Consensus Mechanisms).....	18
3.3.1 Απόδειξη Εργασίας (Proof of Work - PoW).....	18
3.3.2 Απόδειξη Συμμετοχής (Proof of Stake - PoS).....	19
3.4 Ψηφιακά Tokens και Έξυπνα Συμβόλαια (Smart Contracts)	20
3.4.1 Έξυπνα Συμβόλαια (Smart Contracts)	20
3.4.2 Ψηφιακά Tokens και Πρότυπα	20
4. Ανάλυση Εφαρμογών και Κοινωνικοοικονομική Επίδραση	22
4.1 Παρουσίαση Online Εφαρμογών και Πλατφορμών.....	22
4.2 Πρωτόκολλα Αποκεντρωμένης Οικονομίας (Decentralized Finance - DeFi).....	22
4.3 Κοινωνικές Επιπτώσεις και Ζητήματα Ασφάλειας	23
4.3.1 Χρηματοοικονομική Συμπερίληψη και Εκδημοκρατισμός	23
4.3.2 Ιδιωτικότητα vs. Κανονιστική Συμμόρφωση	23
4.3.3 Τεχνολογικές Ευπάθειες και Κίνδυνοι Ασφάλειας	24
5. Προηγμένες Κρυπτογραφικές Υποδομές και Ασφάλεια Δικτύων	26

5.1 Ο Ρόλος της Κρυπτογραφίας σε Περιβάλλοντα Μηδενικής Εμπιστοσύνης (Trustless Environments)	26
5.2 Ασύμμετρη Κρυπτογραφία και Ελλειπτικές Καμπύλες (ECC).....	27
5.2.1 Το Πρόβλημα του Διακριτού Λογαρίθμου (ECDLP) και η Μαθηματική Θεμελίωση.....	27
5.2.2 Συγκριτική Ανάλυση Αποδοτικότητας: RSA έναντι ECC	28
5.3 Μηχανισμοί Ψηφιακών Υπογραφών (Digital Signature Schemes)	29
5.3.1 Ο Αλγόριθμος ECDSA και η Κρίσιμη Ευπάθεια του Τυχαίου Nonce	29
5.3.2 Υπογραφές Schnorr, Ιδιότητα Γραμμικότητας και η Αναβάθμιση Taproot	30
5.4 Διαχείριση Κλειδιών, Ιεραρχικά Ντετερμινιστικά Πορτοφόλια και Πρότυπα BIP ..	30
5.4.1 BIP-32: Ιεραρχικά Ντετερμινιστικά Πορτοφόλια (HD Wallets).....	30
5.4.2 BIP-39: Μνημονικές Φράσεις και Κωδικοποίηση Εντροπίας	31
5.4.3 BIP-44: Πολυ-Νομισματική Οργάνωση (Multi-Account Hierarchy)	31
5.5 Προηγμένες Τεχνικές Ιδιωτικότητας και Ανωνυμίας	32
5.5.1 Αποδείξεις Μηδενικής Γνώσης (Zero-Knowledge Proofs - ZKP)	32
5.5.2 Υπηρεσίες Ανάμειξης (Mixers), Έξυπνα Συμβόλαια και το Tornado Cash ...	33
5.5.3 Υπολογισμός Πολλαπλών Μερών (Multi-Party Computation - MPC)	34
5.6 Η Υπαρξιακή Απειλή των Κβαντικών Υπολογιστών (Y2Q).....	35
6. Προκλήσεις Επεκτασιμότητας, Λύσεις Layer 2 και Διαλειτουργικότητα	36
6.1 Το Τρίλημμα της Επεκτασιμότητας (The Scalability Trilemma)	36
6.2 Λύσεις Πρώτου Επιπέδου (Layer 1 Scaling Solutions).....	37
6.2.1 Αύξηση Μεγέθους Μπλοκ (Block Size Increase) και SegWit.....	37
6.2.2 Τεμαχισμός Βάσης Δεδομένων (Sharding)	37
6.3 Λύσεις Δεύτερου Επιπέδου (Layer 2 Scaling) και Αρθρωτή Αρχιτεκτονική	37
6.3.1 Κανάλια Κατάστασης (State Channels).....	38
6.3.2 Πλευρικές Αλυσίδες (Sidechains) έναντι Πραγματικών Layer 2.....	38
6.3.3 Ο Ρόλος της Διαθεσιμότητας Δεδομένων (Data Availability)	38
6.4 Αρθρωτά Blockchains (Modular Architecture) και Proto-Danksharding.....	39
6.5 Διαλειτουργικότητα και Γέφυρες Δικτύων (Cross-Chain Bridges)	40
6.5.1 Ο Μηχανισμός Lock-and-Mint και ο Συστημικός Κίνδυνος (Honeypot)	40
6.5.2 Μοντέλα Επαλήθευσης (Verification Models) και Μηχανισμοί Ασφαλείας....	40
6.5.3 Οι Αρχιτεκτονικές του Επίπεδου 0 (Layer 0): Cosmos και Polkadot.....	41
7.1 Τοκενοποίηση Πραγματικών Περιουσιακών Στοιχείων (RWA)	43
7.1.1 Τεχνικά Πρότυπα Ασφαλείας: ERC-1400 και ERC-3643	44
7.1.2 Διαφάνεια Αποθεματικών και Proof of Reserve	45
7.2 Το Ευρωπαϊκό Ρυθμιστικό Πλαίσιο MiCA και η Κανονιστική Συμμόρφωση	45
7.3 Ψηφιακά Νομίσματα Κεντρικών Τραπεζών (CBDCs)	46
7.4 Αυτοκυρίαρχη Ταυτότητα (Self-Sovereign Identity - SSI)	47
7.5 Αποκεντρωμένα Δίκτυα Φυσικών Υποδομών (DePIN).....	47
8. Η Οικονομία της Προσοχής: Memecoins, Συμπεριφορική Χρηματοοικονομική και Δυναμική των Αγορών.....	49
8.1 Ιστορική Αναδρομή: Από την Παρωδία στη Βιομηχανία Δισεκατομμυρίων	49

Πτυχιική Εργασία	Ιωάννης Μπαλκούρας
8.2 Τεχνολογική Υποδομή και Μηχανισμοί Ρευστότητας.....	50
8.2.1 Αυτοματοποιημένοι Ειδικοί Διαπραγματευτές (AMMs)	50
8.2.2 Καμπύλες Δέσμευσης (Bonding Curves)	51
8.3 Συμπεριφορική Χρηματοοικονομική και Η Δυναμική του "Day Trading"	52
8.4 Κυβερνοασφάλεια, MEV Bots και Συστημικοί Κίνδυνοι.....	52
8.4.1 Το Φαινόμενο του Rug Pull (Τράβηγμα Χαλιού)	52
8.4.2 Μέγιστη Εξαγωγή Αξία (MEV) και Sniping Bots	53
8.5 Συμπεριφορική Αξιολόγηση και Συμπεράσματα	54
9. Τεχνική Ανάλυση και Αρχιτεκτονική του Προτεινόμενου Πρωτοκόλλου DeFi (Lending Protocol)	55
9.1 Αρχιτεκτονική του Έξυπνου Συμβολαίου και Βιβλιοθήκες	55
9.1.1 Χρήση Ασφαλών Μαθηματικών (SafeMath) και Modifiers	55
9.2 Μηχανισμός Παροχής Ρευστότητας (Liquidity Provision)	56
9.3 Μαθηματικό Μοντέλο Δανεισμού και Υπερ-Εξασφάλιση (Over-collateralization)	57
9.4 Αλγόριθμος Υπολογισμού Υγείας Λογαριασμού (Health Factor)	57
9.5 Μηχανισμός Ρευστοποίησης (Liquidation Process).....	57
10. Μεθοδολογία Βιβλιογραφικής Ανασκόπησης.....	59
10.1 Το Πρωτόκολλο PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses).....	59
10.2 Στρατηγική Αναζήτησης και Βάσεις Δεδομένων (Search Strategy)	59
10.3 Κριτήρια Εισαγωγής και Αποκλεισμού (Inclusion & Exclusion Criteria)	60
10.4 Διαδικασία Επιλογής Μελετών (Study Selection Process)	60
11. Αποτελέσματα, Συζήτηση και Μελλοντικές Τάσεις.....	61
11.1 Σύνθεση Ευρημάτων και η Νέα Ψηφιακή Υποδομή.....	61
11.2 Η Σύγκλιση Τεχνητής Νοημοσύνης (AI) και Blockchain: Η Οικονομία των Αυτόνομων Πρακτόρων.....	61
11.2.1 Το Πρόβλημα των Τραπεζών και οι Αυτόνομοι Πράκτορες (AI Agents)	61
11.2.2 Μηχανική Μάθηση Μηδενικής Γνώσης (zkML)	61
11.2.3 Καταπολέμηση των Deepfakes (Content Authenticity)	62
11.3 Η Μετάβαση στη Μετα-Κβαντική Εποχή (Post-Quantum Transition)	62
11.4 Το Μέλλον της Χρηστικότητας: Αφαίρεση Λογαριασμού (Account Abstraction)	63
12. Συμπεράσματα	64
Πίνακας Ορολογίας	66
Πίνακας Συντημήσεων - Ακρωνυμίων	68
ΒΙΒΛΙΟΓΡΑΦΙΑ (REFERENCES)	69
Παράρτημα Α: Πηγαίος Κώδικας Υλοποίησης Αποκεντρωμένου Πρωτοκόλλου Δανεισμού (DeFi Lending Smart Contract)	73

Κατάλογος Εικόνων

Εικόνα 1: Οπτική αναπαράσταση του Προβλήματος των Βυζαντινών Στρατηγών και της ανταλλαγής αντιφατικών μηνυμάτων (Sybil / Traitor nodes).....	12
Εικόνα 2: Το πρωτοσέλιδο της εφημερίδας The Times (3 Ιανουαρίου 2009) και το ενσωματωμένο μήνυμα του Satoshi Nakamoto στο Genesis Block του Bitcoin.....	14
Εικόνα 3: Λογικό διάγραμμα ροής (Flowchart) και κύκλος ζωής ενός Έξυπνου Συμβολαίου (Smart Contract).....	15
Εικόνα 4: Αρχιτεκτονική δομή και διασύνδεση των Blocks σε ένα κατακεντρωμένο δίκτυο.....	16
Εικόνα 5: Δομή ενός Δέντρου Merkle (Merkle Tree) και ο κρυπτογραφικός κατακερματισμός των συναλλαγών.....	17
Εικόνα 6: Η λειτουργία της μονόδρομης συνάρτησης SHA-256 και το φαινόμενο της χιονοστιβάδας (Avalanche Effect).....	17
Εικόνα 7: Συγκριτική κατανομή της ετήσιας ενεργειακής κατανάλωσης (σε TWh) μεταξύ αποκεντρωμένων δικτύων, εξόρυξης χρυσού και παραδοσιακού τραπεζικού συστήματος.....	19
Εικόνα 8: Συγκριτική αναπαράσταση λειτουργίας των μηχανισμών Απόδειξης Εργασίας (PoW) και Απόδειξης Συμμετοχής (PoS).....	19
Εικόνα 9: Τοπολογική σύγκριση Κεντριοποιημένων και Κατακεντρωμένων συστημάτων δικτύου.....	22
Εικόνα 10: Ροή λειτουργίας ενός Πρωτοκόλλου Αποκεντρωμένου Δανεισμού (DeFi Lending) και μηχανισμός υπερ-εξασφάλισης (Over-collateralization).....	Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.
Εικόνα 11: Εξέλιξη της Συνολικής Κλειδωμένης Αξίας (Total Value Locked - TVL) στα πρωτόκολλα της Αποκεντρωμένης Οικονομίας (DeFi) για την περίοδο 2019-2024.....	23
Εικόνα 12: Μηχανισμός εκτέλεσης μιας επίθεσης επανεισόδου (Reentrancy Attack) σε ένα ευάλωτο Έξυπνο Συμβολαίο προτού ενημερωθεί το λογιστικό του υπόλοιπο.....	Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.
Εικόνα 13: Γραφική αναπαράσταση μιας Ελλειπτικής Καμπύλης (ECC) πάνω στην οποία βασίζεται η ασύμμετρη παραγωγή δημοσίων κλειδιών.....	28
Εικόνα 14: Αρχιτεκτονική διάδρασης μεταξύ Αποδεικνύοντος (Prover) και Επαληθευτή (Verifier) σε ένα πρωτόκολλο Αποδείξεων Μηδενικής Γνώσης (ZKP).....	33
Εικόνα 15: Το Τρίλημμα της Επεκτασιμότητας του Blockchain (Αποκέντρωση, Ασφάλεια, Επεκτασιμότητα).....	36
Εικόνα 16: Τοπολογική δομή και μετατόπιση του υπολογιστικού φόρτου από το Βασικό Δίκτυο (Layer 1) στις λύσεις Δεύτερου Επιπέδου (Rollups).....	39
Εικόνα 17: Τα στάδια ψηφιοποίησης και τοκενοποίησης Πραγματικών Περιουσιακών Στοιχείων (RWA) και η διασύνδεσή τους με τα αποκεντρωμένα δίκτυα.....	43
Εικόνα 18: Το «Τρίγωνο Εμπιστοσύνης» της Αυτοκυρίαρχης Ταυτότητας (SSI) και η αποκεντρωμένη ανταλλαγή Επαληθεύσιμων Διαπιστευτηρίων.....	47
Εικόνα 19: Μαθηματική αναπαράσταση μιας Καμπύλης Δέσμευσης (Bonding Curve) για τον αλγοριθμικό καθορισμό της τιμής βάσει προσφοράς και ζήτησης.....	51
Εικόνα 20: Μηχανισμός εκτέλεσης επίθεσης τύπου "Sandwich" από αλγόριθμους Μέγιστης Εξαγωγίμις Αξίας (MEV Bots) στο Mempool του δικτύου.....	54
Εικόνα 21: Μηχανισμός εκτέλεσης επίθεσης τύπου "Sandwich" από αλγόριθμους Μέγιστης Εξαγωγίμις Αξίας (MEV Bots) στο Mempool του δικτύου 2.....	54
Εικόνα 22: Οπτική αναπαράσταση του μηχανισμού παροχής ρευστότητας (Liquidity Provision) και της συγκρότησης μιας Δεξαμενής Ρευστότητας (Liquidity Pool) στο πλαίσιο λειτουργίας των Αυτοματοποιημένων Ειδικών Διαπραγματευτών (AMMs).....	56
Εικόνα 23: Διάγραμμα ροής της αλγοριθμικής διαδικασίας Ρευστοποίησης (Liquidation). Απεικονίζεται η παρέμβαση των εξωτερικών εκκαθαριστών (Liquidation Bots) για την εξόφληση του χρέους, όταν ο Δείκτης Υγείας (Health Factor) υποχωρήσει κάτω από τη μονάδα.....	58

1. Εισαγωγή

Το φθινόπωρο του 2008, η παγκόσμια οικονομία βρέθηκε αντιμέτωπη με τη μεγαλύτερη συστημική κατάρρευση από την εποχή του Μεγάλου Κραχ του 1929. Η πτώχευση κολοσσών όπως η Lehman Brothers και η επακόλουθη κρίση ενυπόθηκων δανείων, κατέδειξαν με τον πλέον δραματικό τρόπο τις δομικές παθογένειες ενός υπερ-συγκεντρωτικού χρηματοπιστωτικού συστήματος. Σε αυτό το περιβάλλον ακραίας αβεβαιότητας και πλήρους κλονισμού της εμπιστοσύνης προς τους παραδοσιακούς θεσμούς, δημοσιεύτηκε σε μια λίστα αλληλογραφίας κρυπτογράφων (cryptography mailing list) ένα ολιγοσέλιδο, αλλά ρηξικέλευθο ακαδημαϊκό κείμενο (whitepaper).

Ο συγγραφέας του, υπό το ψευδώνυμο Satoshi Nakamoto, δεν πρότεινε απλώς άλλη μια θεωρητική μορφή ηλεκτρονικού χρήματος, αλλά παρουσίασε την πρώτη, ιστορικά εφαρμόσιμη αρχιτεκτονική του Blockchain. Επρόκειτο για το Bitcoin: ένα δίκτυο ομότιμης αρχιτεκτονικής (peer-to-peer), ικανό να διασφαλίσει τη μεταφορά αξίας σε ένα περιβάλλον «μηδενικής εμπιστοσύνης» (trustless), καταργώντας οριστικά την ανάγκη για ενδιάμεσα καταπιστεύματα, όπως οι κεντρικές τράπεζες ή οι κρατικοί εκκαθαριστικοί φορείς.

Η καινοτομία αυτή, ωστόσο, δεν προέκυψε εν κενώ. Αποτέλεσε το αποκορύφωμα δεκαετιών ακαδημαϊκής έρευνας στην επιστήμη της πληροφορικής, ενσωματώνοντας θεωρίες από το κίνημα των "Cypherpunks" της δεκαετίας του 1990. Πρόδρομες προσπάθειες, όπως το eCash του David Chaum, το Hashcash του Adam Back, το b-money του Wei Dai και το Bit Gold του Nick Szabo, είχαν θέσει τα θεωρητικά θεμέλια. Ο Nakamoto κατάφερε να συνθέσει αυτά τα κρυπτογραφικά εργαλεία με τη Θεωρία Παιγνίων (Game Theory), επιλύοντας μαθηματικά προβλήματα που ταλάνιζαν την επιστήμη των κατανεμημένων συστημάτων για δεκαετίες.

Η βαρύτητα της παρούσας πτυχιακής εργασίας έγκειται ακριβώς στην επιτακτική ανάγκη κατανόησης αυτών των τεχνολογικών πυλώνων. Σε μια εποχή όπου ο ψηφιακός μετασχηματισμός επαναπροσδιορίζει κάθε πτυχή του κοινωνικού και οικονομικού βίου, η εις βάθος μελέτη κρυπτογραφικών μηχανισμών —όπως οι συναρτήσεις κατακερματισμού (hashing), η ασύμμετρη κρυπτογραφία και η αρχιτεκτονική των Κατανεμημένων Καθολικών (Distributed Ledgers)— δεν συνιστά απλώς μια θεωρητική άσκηση. Αντιθέτως, αποτελεί απαραίτητο εφόδιο για τον σύγχρονο επιστήμονα της πληροφορικής, ο οποίος καλείται να σχεδιάσει και να αξιολογήσει τις υποδομές της επόμενης γενιάς του διαδικτύου.

1.1 Το Πλαίσιο της Αποκεντρωμένης Τεχνολογίας και το Web3

Για να γίνει πλήρως αντιληπτό το μέγεθος αυτής της τεχνολογικής τομής, οφείλουμε να ανατρέξουμε στην εξελικτική πορεία του ίδιου του Παγκόσμιου Ιστού. Στα πρώτα του βήματα (Web 1.0), κατά τη δεκαετία του 1990, το διαδίκτυο λειτούργησε αυστηρά ως ένας στατικός, αποκεντρωμένος μεν, αλλά μονοδιάστατος χώρος ανάγνωσης πληροφοριών (read-only). Βασιζόταν σε ανοιχτά πρωτόκολλα (όπως το HTTP και το SMTP), τα οποία δεν ανήκαν σε καμία εταιρεία.

Η μετάβαση στο Web 2.0, στις αρχές της χιλιετίας, έφερε την πολυπόθητη διαδραστικότητα (read-write), επιτρέποντας στους χρήστες να παράγουν και να διαμοιράζονται περιεχόμενο. Εντούτοις, αυτό το μοντέλο εξελίχθηκε σε αυτό που η σύγχρονη ακαδημαϊκή κοινότητα ονομάζει «πλατφορμικό καπιταλισμό». Η αρχιτεκτονική στηρίχθηκε στην απόλυτη κυριαρχία λίγων τεχνολογικών κολοσσών (Big Tech), οι οποίοι αντικατέστησαν τα ανοιχτά πρωτόκολλα με κλειστά οικοσυστήματα (walled gardens). Σήμερα, αυτές οι οντότητες λειτουργούν ως κεντρικοί διαχειριστές και απόλυτοι θεματοφύλακες (gatekeepers) των δεδομένων, ελέγχοντας πλήρως την ψηφιακή ταυτότητα των χρηστών και δημιουργώντας επικίνδυνα Κεντρικά Σημεία Αποτυχίας (Single Points of Failure), τόσο σε επίπεδο κυβερνοασφάλειας όσο και σε επίπεδο προστασίας προσωπικών δεδομένων.

Αντίστοιχα, στον χρηματοοικονομικό τομέα, η παγκόσμια αρχιτεκτονική παρέμεινε εξίσου, αν όχι περισσότερο, συγκεντρωτική. Το Παραδοσιακό Χρηματοπιστωτικό Σύστημα (Traditional Finance - TradFi) βασίζεται αποκλειστικά σε κλειστές, εταιρικές βάσεις δεδομένων (silos). Μολονότι το σύστημα αυτό υποστήριξε την ανάπτυξη της παγκόσμιας οικονομίας, οι εγγενείς αδυναμίες του είναι πλέον αδιαμφισβήτητες: υπέρογκα κόστη συντήρησης, αδιαφανείς διαδικασίες, πολυήμερες καθυστερήσεις στις διασυνωριακές εκκαθαρίσεις (μέσω συστημάτων

όπως το SWIFT) και αποκλεισμός δισεκατομμυρίων ανθρώπων (unbanked population) από βασικές τραπεζικές υπηρεσίες.

Σε αυτό το κρίσιμο τεχνολογικό μεταίχμιο, η αρχιτεκτονική του Blockchain προσέφερε μια ριζοσπαστική διέξοδο. Ενώ το Bitcoin απέδειξε ότι ένα παγκόσμιο δίκτυο μπορεί να διατηρήσει ένα κοινό καθολικό ασφαλές, η πραγματική έκρηξη στην επιστήμη των υπολογιστών σημειώθηκε το 2015 με την έλευση του δικτύου Ethereum. Μετατρέποντας το blockchain από ένα απλό σύστημα μεταφοράς νομισμάτων σε έναν παγκόσμιο, κατακεντρωμένο υπολογιστή (Turing-complete state machine), το Ethereum εισήγαγε τα Έξυπνα Συμβόλαια (Smart Contracts). Αυτοί οι αυτόνομοι, αμετάβλητοι προγραμματιστικοί κώδικες έθεσαν τα θεμέλια του Web 3.0 (read-write-own). Δημιούργησαν ένα διαδίκτυο όπου η αξία και η ιδιοκτησία μεταφέρονται εγγενώς, οδηγώντας στη γέννηση της Αποκεντρωμένης Χρηματοοικονομικής (DeFi) — ενός οικοσυστήματος που αναδιαμορφώνει πλήρως τις τραπεζικές υπηρεσίες μέσω διαφανούς, ανοιχτού κώδικα (open-source).

1.2 Κίνητρο και Σκοπός της Πτυχιακής Εργασίας

Το κύριο έναυσμα για την εκπόνηση της παρούσας διπλωματικής εργασίας προέκυψε από την ανάγκη να γεφυρωθεί το τεράστιο χάσμα που παρατηρείται μεταξύ της θεωρητικής, ακαδημαϊκής προσέγγισης του Blockchain και της πρακτικής, βιομηχανικής του εφαρμογής. Παρατηρείται συχνά το φαινόμενο, ένα μεγάλο μέρος της σύγχρονης αρθρογραφίας αλλά και της κοινής γνώμης, να αναλώνεται σχεδόν εμμονικά στην κερδοσκοπική φύση των κρυπτονομισμάτων και στις ακραίες διακυμάνσεις των τιμών τους. Η επιφανειακή αυτή προσέγγιση παραβλέπει συστηματικά τη βαθύτερη, εξαιρετικά σύνθετη αλγοριθμική δομή που βρίσκεται στον πυρήνα αυτών των συστημάτων.

Ως φοιτητής Πληροφορικής, ο πρωταρχικός σκοπός μου μέσω αυτής της εργασίας είναι η εις βάθος τεχνική αποδόμηση των υποκείμενων τεχνολογιών του οικοσυστήματος. Η παρούσα μελέτη δεν αρκείται σε μια περιγραφική ιστορική αναδρομή. Αντιθέτως, επιχειρεί να ρίξει φως «κάτω από το καπνό» (under the hood): να αναλύσει τον κώδικα, να εξετάσει την πολυπλοκότητα των πρωτοκόλλων συναίνεσης (Consensus Protocols) και να κατανοήσει πώς διασφαλίζεται η ακεραιότητα των δεδομένων μέσα από δομές όπως τα Δέντρα Merkle (Merkle Trees) και τα πρωτόκολλα Αποδείξεων Μηδενικής Γνώσης (ZK-Proofs).

Επιπροσθέτως, η εργασία στοχεύει να αποδείξει την ωριμότητα της Αποκεντρωμένης Χρηματοοικονομικής (DeFi) σε αυστηρά εφαρμοσμένο, προγραμματιστικό επίπεδο. Για τον λόγο αυτό, αρνήθηκα να περιοριστώ σε μια απλή βιβλιογραφική ανασκόπηση, αλλά προχώρησα στην πρακτική υλοποίηση ενός λειτουργικού συστήματος. Μέσω της συγγραφής ενός Αποκεντρωμένου Πρωτοκόλλου Δανεισμού σε γλώσσα προγραμματισμού Solidity —ο πλήρης, τεκμηριωμένος κώδικας του οποίου παρατίθεται στο Παράρτημα της εργασίας— επιχειρώ να καταδείξω πώς η αφηρημένη θεωρία της κρυπτογραφίας μετατρέπεται σε διαφανή, αδιάφθορο και εκτελέσιμο κώδικα, ικανό να αντικαταστήσει τους παραδοσιακούς πιστωτικούς μηχανισμούς δισεκατομμυρίων δολαρίων.

1.3 Διάρθρωση της Πτυχιακής

Προκειμένου να καλυφθεί ομαλά και συνεκτικά το εύρος του γνωστικού αντικειμένου, η παρούσα πτυχιακή εργασία αναπτύσσεται οργανικά σε διακριτά κεφάλαια, σύμφωνα με την ακόλουθη δομή:

- **Κεφάλαια 1 έως 4:** Αναλύεται το ιστορικό υπόβαθρο, η μετάβαση στο Web 3.0 και το θεωρητικό πλαίσιο των ψηφιακών νομισμάτων.
- **Κεφάλαιο 5 (Κρυπτογραφία):** Εμβαθύνει στον πυρήνα της Επιστήμης Υπολογιστών, αναλύοντας τις συναρτήσεις κατακερματισμού, την Κρυπτογραφία Ελλειπτικών Καμπυλών (ECC) και τις Αποδείξεις Μηδενικής Γνώσης (ZKPs).
- **Κεφάλαιο 6 (Λύσεις Κλιμάκωσης):** Προσεγγίζει το θεμελιώδες Τρίλημμα του Blockchain και εξετάζει τεχνικά τις σύγχρονες Λύσεις Δεύτερου Επιπέδου (Layer-2 Rollups) και τα πρωτόκολλα διαλειτουργικότητας.

- **Κεφάλαια 7 έως 9 (Εφαρμογές και Tokenomics):** Εξετάζεται η Τοκενοποίηση Πραγματικών Περιουσιακών Στοιχείων (RWAs), τα δίκτυα DePIN και η συμπεριφορική οικονομία πίσω από τα Memecoins και τους μηχανισμούς AMM.
- **Κεφάλαια 10 έως 12:** Συνοψίζονται τα Case Studies αποτυχιών του κλάδου (όπως τα φαινόμενα Rug Pulls και η κατάρρευση κεντρικών ανταλλακτηρίων) και η εργασία ολοκληρώνεται με τη διατύπωση των τελικών συμπερασμάτων.
- **Παράρτημα Α:** Παρατίθεται αναλυτικά ο πηγαίος κώδικας του Έξυπνου Συμβολαίου Δανεισμού (DeFi Lending Smart Contract) σε γλώσσα Solidity, συνοδευόμενος από τον αντίστοιχο προγραμματιστικό σχολιασμό.

1.4 Το Πρόβλημα των Βυζαντινών Στρατηγών (Byzantine Generals Problem)

Η βαθύτερη κατανόηση της τεχνολογικής επανάστασης που επέφερε το Blockchain προϋποθέτει, αναπόφευκτα, την εξέταση του κεντρικού μαθηματικού προβλήματος που το σύστημα αυτό κλήθηκε να επιλύσει. Στην επιστήμη των κατακευματισμένων συστημάτων (distributed systems), η πλέον δυσεπίλυτη πρόκληση σχετίζεται άμεσα με το Θεώρημα CAP, το οποίο δηλώνει ότι ένα κατακευματισμένο σύστημα δεδομένων δεν μπορεί να εγγυηθεί ταυτόχρονα τη Συνέπεια (Consistency), τη Διαθεσιμότητα (Availability) και την Ανοχή στην Κατάτμηση (Partition Tolerance).

Η αναζήτηση της επίτευξης ομοφωνίας (consensus) μεταξύ ανεξάρτητων, απομακρυσμένων κόμβων, όταν απουσιάζει παντελώς μια κεντρική ελεγκτική αρχή, διατυπώθηκε επισήμως το 1982 από τους ερευνητές Leslie Lamport, Robert Shostak και Marshall Pease. Στην ακαδημαϊκή βιβλιογραφία, το θεωρητικό αυτό αδιέξοδο καταγράφηκε ως το «Πρόβλημα των Βυζαντινών Στρατηγών».

1.4.1 Η Θεωρητική Αλληγορία και ο Ορισμός του Προβλήματος

Για την οπτικοποίηση της πολυπλοκότητας του προβλήματος, οι ερευνητές χρησιμοποίησαν μια ευφυή ιστορική αλληγορία (βασισμένη στο παλαιότερο "Πρόβλημα των Δύο Στρατηγών"). Υποτίθεται ότι μια ομάδα στρατηγών του Βυζαντινού στρατού έχει περικυκλώσει μια εχθρική πόλη, παραμένοντας σταθμευμένοι σε διαφορετικά, απομακρυσμένα στρατόπεδα. Ελλείψει σύγχρονων τηλεπικοινωνιών, η μόνη μέθοδος συγχρονισμού μεταξύ τους είναι η αποστολή αγγελιαφόρων μέσα από εχθρικά εδάφη.

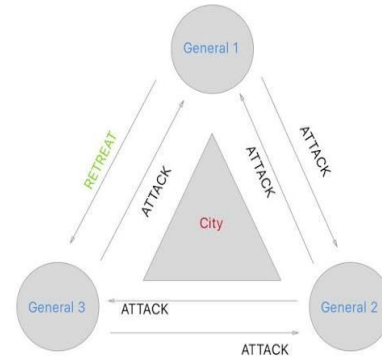
Για να αποφευχθεί η συντριβή, όλοι οι στρατηγοί οφείλουν να καταλήξουν σε ένα απολύτως κοινό σχέδιο δράσης: είτε ολομέτωπη επίθεση ταυτόχρονα, είτε καθολική υποχώρηση. Μια ασυντόνιστη κίνηση (π.χ. οι μισοί να επιτεθούν και οι μισοί να υποχωρήσουν) θα αποβεί μοιραία για ολόκληρο το στράτευμα. Η υπολογιστική πολυπλοκότητα, συνεπώς, προκύπτει από δύο τεράστιους αστάθμητους παράγοντες:

1. **Η Αξιοπιστία του Διαύλου Επικοινωνίας (Network Reliability):** Οι αγγελιαφόροι ενδέχεται να αιχμαλωτιστούν, να καθυστερήσουν ή να δολοφονηθούν, προκαλώντας ανεπανόρθωτη απώλεια μηνυμάτων. Αυτό αποτελεί την τέλεια θεωρητική προσομοίωση της απώλειας πακέτων (packet loss) ή των προβλημάτων καθυστέρησης (latency) σε ένα δίκτυο TCP/IP.
2. **Η Παρουσία Κακόβουλων Δρώντων (Malicious Actors):** Είναι μαθηματικά βέβαιο ότι ανάμεσα στους στρατηγούς υπάρχουν «προδότες». Αυτοί θα αποστείλουν εσκεμμένα αντιφατικά μηνύματα (π.χ. στον Στρατηγό Α θα διατάξουν επίθεση και στον Στρατηγό Β υποχώρηση), με μοναδικό σκοπό να προκαλέσουν επιχειρησιακό χάος. Αυτό προσομοιώνει άριστα τους hackers, τους παραβιασμένους υπολογιστές ή τους ελαττωματικούς κόμβους ενός δικτύου.

1.4.2 Βυζαντινή Ανοχή Σφαλμάτων (Byzantine Fault Tolerance - BFT)

Η ανθεκτικότητα ενός συστήματος —δηλαδή η ικανότητά του να συνεχίζει να λειτουργεί ορθά και να επιτυγχάνει αδιάψευστη συναίνεση, παρά την ενεργή δράση «προδοτών»— ονομάζεται Βυζαντινή Ανοχή Σφαλμάτων (Byzantine Fault Tolerance - BFT).

Ιστορικά και μαθηματικά, αποδείχθηκε ότι σε ένα παραδοσιακό δίκτυο, για να επιτευχθεί συναίνεση και να απομονωθούν m κακόβουλοι κόμβοι, το σύστημα απαιτεί την ύπαρξη τουλάχιστον $3m + 1$ συνολικών κόμβων. Πρακτικά, αυτό σημαίνει ότι ένα δίκτυο θεωρείται ασφαλές μόνο εάν οι παραβιασμένοι κόμβοι αντιπροσωπεύουν αυστηρά λιγότερο από το 33% (1/3) του συνολικού πληθυσμού. Εντούτοις, η λύση αυτή προϋπέθετε ένα κλειστό περιβάλλον (permissioned network), όπου όλοι οι συμμετέχοντες είναι γνωστοί. Στο σύγχρονο, ανοιχτό διαδίκτυο, η ταυτότητα ενός κόμβου μπορεί να πλαστογραφηθεί με τεράστια ευκολία. Ένας επιτιθέμενος θα μπορούσε να δημιουργήσει χιλιάδες εικονικούς κόμβους (Sybil Attack) και να υπερβεί άμεσα το όριο προστασίας του 33%



Εικόνα 1: Οπτική αναπαράσταση του Προβλήματος των Βυζαντινών Στρατηγών και της ανταλλαγής αντιφατικών μηνυμάτων (Sybil / Traitor nodes)

1.4.3 Η Λύση του Satoshi Nakamoto: Proof of Work και Οικονομικά Κίνητρα

Το ιδιοφυές επίτευγμα του Bitcoin, και κατ' επέκταση του συνόλου της βιομηχανίας του Blockchain, ήταν ότι προσέφερε την πρώτη πρακτικά εφαρμόσιμη, βιομηχανικά κλιμακώσιμη λύση σε αυτό το πρόβλημα δεκαετιών, λειτουργώντας σε πλήρως ανοιχτά, αποκεντρωμένα δίκτυα (permissionless networks), όπου ο καθένας μπορεί να συμμετάσχει διατηρώντας την ανωνυμία του.

Ο Nakamoto δεν επιχείρησε να αντικρούσει τα θεωρητικά μαθηματικά του 33%. Αντιθέτως, γεφύρωσε με μοναδικό τρόπο την επιστήμη των υπολογιστών με τη Θεωρία Παιγνίων (Game Theory) και τα εφαρμοσμένα μακροοικονομικά. Εισάγοντας τον αλγόριθμο της Απόδειξης Εργασίας (Proof of Work), έθεσε έναν απαραίτητο, φυσικό κανόνα στο ψηφιακό οικοσύστημα: προκειμένου ένας «στρατηγός» (κόμβος / εξορύκτης) να αποκτήσει το δικαίωμα να μιλήσει και να προσθέσει ένα νέο μπλοκ δεδομένων στο καθολικό, οφείλει προηγουμένως να αποδείξει μαθηματικά στο υπόλοιπο δίκτυο ότι κατανάλωσε τεράστια, πραγματική υπολογιστική ισχύ (χρόνο επεξεργαστών ASICs) και, κατ' επέκταση, τεράστια ποσά ηλεκτρικής ενέργειας.

Αυτή η σύνδεση του ψηφιακού κώδικα με τη θερμοδυναμική του πραγματικού κόσμου κατέστησε τη δημιουργία χιλιάδων ψεύτικων ταυτοτήτων (Sybil Attacks) οικονομικά εντελώς απαγορευτική, καθώς κάθε «ψεύτικος» στρατηγός απαιτεί πλέον πανάκριβο εξοπλισμό και ρεύμα για να υπάρξει.

Παράλληλα, το σύστημα ενσωμάτωσε θετικά οικονομικά κίνητρα (block rewards & transaction fees). Οι κόμβοι ανταμείβονται με νεοεκδοθέντα κρυπτονομίσματα αποκλειστικά και μόνο όταν προσθέτουν στο δίκτυο αληθή δεδομένα συναλλαγών, με τα οποία συμφωνεί η απόλυτη πλειοψηφία (Longest Chain Rule). Σε περίπτωση που ένας κόμβος αποπειραθεί να παραποιήσει τις συναλλαγές και να συμπεριφερθεί κακόβουλα, το δίκτυο εντοπίζει άμεσα την ανακολουθία στα Hash και απορρίπτει το μπλοκ του. Το αποτέλεσμα είναι ο κακόβουλος χρήστης να υποστεί τεράστια, άμεση οικονομική ζημία λόγω του σπαταλημένου ρεύματος, χωρίς καμία ανταμοιβή. Σε τελική ανάλυση, η αρχιτεκτονική του Blockchain επέλυσε το Πρόβλημα των Βυζαντινών Στρατηγών ευθυγραμμίζοντας απόλυτα τα κίνητρα, καθιστώντας την εντιμότητα και τη συνεργασία μαθηματικά και οικονομικά πολύ πιο επικερδή από την προδοσία.

2. Ιστορική Αναδρομή και το Κίνημα των Cypherpunks

Είναι ένα συχνό λάθος να πιστεύει κανείς ότι το Bitcoin εμφανίστηκε ξαφνικά από το πουθενά το 2008. Στην πραγματικότητα, η ιδέα ενός αποκεντρωμένου, ψηφιακού νομίσματος αποτελούσε το «Άγιο Δισκοπότηρο» της επιστήμης της κρυπτογραφίας για περισσότερες από τρεις δεκαετίες. Για να κατανοήσουμε τον τεχνολογικό πυρήνα του Blockchain, οφείλουμε να γυρίσουμε τον χρόνο πίσω και να εξετάσουμε τις ομάδες και τα πειράματα που έστρωσαν το έδαφος.

2.1 Το Κίνημα των Cypherpunks: Η Κρυπτογραφία ως Κοινωνικό Εργαλείο

Στα τέλη της δεκαετίας του 1980 και στις αρχές του 1990, το ίντερνέτ άρχισε να μπαίνει σταδιακά στα σπίτια των απλών χρηστών. Μαζί του όμως ήρθε και ένας πρωτοφανής κίνδυνος: η μαζική παρακολούθηση των δεδομένων.

Εκείνη την περίοδο, μια ομάδα από χαρισματικούς προγραμματιστές, μαθηματικούς και ακτιβιστές της ιδιωτικότητας άρχισε να επικοινωνεί μέσω μιας ηλεκτρονικής λίστας αλληλογραφίας (mailing list). Η ομάδα αυτή ονομάστηκε Cypherpunks (ένα λογοπαίγνιο μεταξύ της λέξης *cipher*, που σημαίνει κρυπτογράφηση, και του κινήματος *cyberpunk*). Βασική τους πεποίθηση ήταν ότι η προστασία της ιδιωτικότητας στην ψηφιακή εποχή δεν πρόκειται να χαριστεί από καμία κυβέρνηση ή εταιρεία, αλλά πρέπει να επιβληθεί τεχνολογικά, γράφοντας κώδικα.

Όπως έγραψε ο Eric Hughes το 1993 στο περίφημο «Μανιφέστο ενός Cypherpunk» (A Cypherpunk's Manifesto): *"Η ιδιωτικότητα είναι απαραίτητη για μια ανοιχτή κοινωνία στην ηλεκτρονική εποχή... Εμείς οι Cypherpunks είμαστε αφοσιωμένοι στο να χτίζουμε ανώνυμα συστήματα. Γράφουμε κώδικα."* Οι Cypherpunks συνειδητοποίησαν κάτι πολύ βασικό: όση κρυπτογράφηση και αν χρησιμοποιείς στα μηνύματά σου, αν οι οικονομικές σου συναλλαγές ελέγχονται από μια κεντρική τράπεζα που παρακολουθεί πού και πότε ξοδεύεις τα χρήματά σου, δεν έχεις πραγματική ελευθερία. Το επόμενο λογικό βήμα ήταν η δημιουργία ενός ψηφιακού νομίσματος πέρα από κρατικό έλεγχο.

2.2 Οι Πρόδρομοι του Ψηφιακού Χρήματος: Τα Αποτυχημένα (αλλά κρίσιμα) Πειράματα

Η προσπάθεια κατασκευής ψηφιακού νομίσματος ήταν γεμάτη αποτυχίες, οι οποίες όμως έδωσαν στον Satoshi Nakamoto τα απαραίτητα "κομμάτια" του παζλ. Τα σημαντικότερα ορόσημα ήταν:

1. Το DigiCash του David Chaum (1989): Ο Chaum ήταν ένας πρωτοπόρος κρυπτογράφος που εφηύρε τις τυφλές υπογραφές. Το DigiCash επέτρεπε ανώνυμες συναλλαγές, αλλά είχε ένα μοιραίο ελάττωμα: ήταν ένα κεντροποιημένο σύστημα. Όταν η εταιρεία του Chaum χρεοκόπησε στα τέλη των 90s, το δίκτυο απλά έκλεισε. Ήταν το πρώτο μεγάλο μάθημα ότι το ψηφιακό χρήμα δεν πρέπει να εξαρτάται από καμία εταιρεία.
2. Το Hashcash του Adam Back (1997): Το Hashcash δεν φτιάχτηκε για νόμισμα, αλλά για την καταπολέμηση του email spam. Απαιτούσε από τον υπολογιστή του αποστολέα να λύσει έναν μικρό μαθηματικό γρίφο πριν στείλει ένα email (ξοδεύοντας ελάχιστη CPU). Αυτή η ιδέα ήταν επαναστατική. Ονομάστηκε *Proof of Work* (Απόδειξη Εργασίας) και, μια δεκαετία αργότερα, έγινε ο ακρογωνιαίος λίθος της ασφάλειας του δικτύου του Bitcoin.
3. Το b-money του Wei Dai (1998) και το Bit Gold του Nick Szabo (2005): Και οι δύο αυτοί ερευνητές προσπάθησαν να φτιάξουν ψηφιακά νομίσματα χωρίς κεντρικό έλεγχο, χρησιμοποιώντας αλυσίδες κρυπτογραφίας (cryptographic chains) και PoW. Δυστυχώς, κανένα από τα δύο δεν κατάφερε να λύσει οριστικά το "Πρόβλημα της Διπλής Δαπάνης" (Double-Spending Problem) χωρίς να χρειαστεί έστω και μια ελάχιστη κεντρική συντονιστική αρχή.

2.3 Η Οικονομική Κρίση του 2008 και το Genesis Block

Το 2008, το παγκόσμιο τραπεζικό σύστημα κατέρρευσε. Οι μεγάλες τράπεζες της Wall Street, έχοντας πάρει τεράστια ρίσκα με χρήματα καταθετών (subprime mortgages), βρέθηκαν στο χείλος

Πτυχιακή Εργασία
της πτώχευσης και διασώθηκαν με κρατικά χρήματα (bailouts) που επιβάρυναν τους φορολογούμενους.

Μέσα σε αυτό το κλίμα βαθιάς δυσπιστίας προς τους παραδοσιακούς θεσμούς, τον



Εικόνα 2: Το πρωτοσέλιδο της εφημερίδας *The Times* (3 Ιανουαρίου 2009) και το ενσωματωμένο μήνυμά του Satoshi Nakamoto στο Genesis Block του Bitcoin.

Ιανουάριο του 2009. Το μήνυμα ήταν ο τίτλος της εφημερίδας *The Times* εκείνης της ημέρας: "*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*". Δεν επρόκειτο απλά για μια χρονοσφραγίδα, αλλά για μια σαφή πολιτική δήλωση.

Οκτώβριο του 2008, ένας άγνωστος προγραμματιστής με το ψευδώνυμο Satoshi Nakamoto (ο οποίος ήταν ενεργό μέλος στη mailing list των Cypherpunks) δημοσίευσε ένα *whitepaper* εννέα σελίδων με τίτλο: "*Bitcoin: A Peer-to-Peer Electronic Cash System*".

Ο Nakamoto κατάφερε αυτό που προσπαθούσαν οι προηγούμενοι για χρόνια: συνδύασε το Proof of Work (του Hashcash), την ασύμμετρη κρυπτογραφία δημοσίου κλειδιού, και ένα αμετάβλητο δημόσιο καθολικό (το Blockchain), δημιουργώντας επιτέλους ένα σύστημα ψηφιακής σπανιότητας χωρίς κανέναν απολύτως διαχειριστή. Το πόσο στενά συνδεδεμένο ήταν το Bitcoin με την αποτυχία του παραδοσιακού συστήματος, αποδεικνύεται από ένα κρυφό μήνυμα που ενσωμάτωσε ο Satoshi στο πρώτο block του δικτύου (Genesis Block) τον

2.4 Η Εξέλιξη: Από το Απλό Χρήμα στα Προγραμματιζόμενα Συμβόλαια (Smart Contracts)

Αν και το Bitcoin πέτυχε απόλυτα τον αρχικό του σκοπό ως ένα ασφαλές, αποκεντρωμένο δίκτυο μεταφοράς αξίας, από πλευράς προγραμματισμού ήταν σχεδιασμένο να είναι εξαιρετικά "δύσκαμπτο". Η εγγενής γλώσσα προγραμματισμού του (το λεγόμενο Bitcoin Script) ήταν επίτηδες περιορισμένη. Πιο συγκεκριμένα, δεν υποστήριζε εντολές βρόχου (loops), καθιστώντας την "Turing-incomplete" (μη-πλήρη κατά Turing).

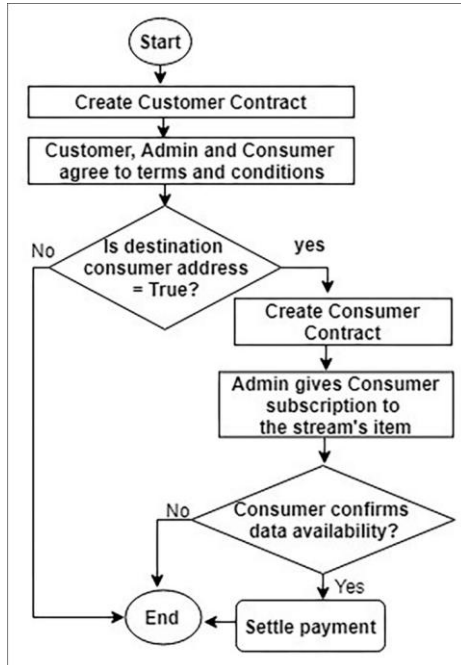
Για να καταλάβουμε γιατί συνέβη αυτό, δεν επρόκειτο για κάποια παράλειψη του Satoshi Nakamoto, αλλά για μια συνειδητή επιλογή ασφαλείας. Αφαιρώντας τα loops, μηδένιζε την πιθανότητα κάποιος κακόβουλος χρήστης να γράψει έναν κώδικα που θα εκτελείται στο άπειρο, κάτι που θα "κόλλαγε" τους υπολογιστές όλων των κόμβων του δικτύου. Έτσι το Bitcoin παρέμεινε απλό: μπορούσε να επιβεβαιώσει ότι ο χρήστης Α έστειλε Χ νομίσματα στον χρήστη Β, αλλά αδυνατούσε να εκτελέσει περίπλοκη επιχειρηματική λογική.

Αυτός ο περιορισμός άρχισε να γίνεται εμπόδιο όσο η τεχνολογία ωρίμαζε. Η ιδέα ότι το blockchain θα μπορούσε να κάνει πολλά περισσότερα από το να είναι απλώς ένα ψηφιακό λογιστικό βιβλίο, άρχισε να κερδίζει έδαφος. Το 2013, ένας νεαρός προγραμματιστής με το όνομα Vitalik Buterin, ο οποίος αρθρογραφούσε στο Bitcoin Magazine, συνειδητοποίησε ότι χρειαζόμασταν μια εντελώς νέα αρχιτεκτονική. Η πρότασή του ήταν το Ethereum, το οποίο κυκλοφόρησε τελικά το 2015 και άλλαξε τα πάντα.

Το Ethereum δεν ήταν απλά άλλο ένα κρυπτονόμισμα, αλλά μια τεράστια αλλαγή παραδείγματος (paradigm shift). Κράτησε τη βασική υποδομή του blockchain (το αποκεντρωμένο δίκτυο και την κρυπτογραφία), αλλά πρόσθεσε στον πυρήνα του μια πλήρη εικονική μηχανή, την Ethereum Virtual Machine (EVM). Αυτό το φαινομενικά μικρό βήμα μετέτρεψε το δίκτυο από ένα "καταμεμημένο καθολικό" σε έναν "παγκόσμιο καταμεμημένο υπολογιστή" (world computer). Πλέον, το σύστημα δεν κατέγραφε μόνο οικονομικά υπόλοιπα, αλλά παρακολουθούσε την

κατάσταση (state) ολόκληρων προγραμμάτων.

Η EVM, πλέον Turing-complete, έδωσε τη δυνατότητα στους προγραμματιστές να γράφουν τα λεγόμενα Έξυπνα Συμβόλαια (Smart Contracts). Ο όρος αυτός είχε επινοηθεί τη δεκαετία του '90 από τον επιστήμονα της πληροφορικής Nick Szabo, αλλά μόλις με το Ethereum βρήκε το περιβάλλον για να υλοποιηθεί πρακτικά. Τα έξυπνα συμβόλαια είναι απλά κομμάτια κώδικα (backend scripts) που ανεβαίνουν στο blockchain και εκτελούνται εντελώς αυτόματα όταν πληρούνται συγκεκριμένες προϋποθέσεις, χωρίς να χρειάζονται κανέναν ενδιάμεσο για να τα επικυρώσει.



Εικόνα 3: Λογικό διάγραμμα ροής (Flowchart) και κύκλος ζωής ενός Έξυπνου Συμβολαίου (Smart Contract).

Το μεγάλο στοίχημα, ωστόσο, ήταν πώς θα προστατευτεί ένα τέτοιο Turing-complete δίκτυο από το περίφημο Πρόβλημα Τερματισμού (Halting Problem) της πληροφορικής. Πώς σταματάς έναν ατέρμονο βρόχο (infinite loop) που θα κατέρρεε το δίκτυο; Η ευφυής λύση του Ethereum ήταν η εισαγωγή του Gas. Κάθε υπολογιστική πράξη που εκτελεί η EVM έχει ένα συγκεκριμένο κόστος σε Gas. Όταν ένας χρήστης ζητά την εκτέλεση ενός έξυπνου συμβολαίου, προπληρώνει ένα όριο (Gas Limit). Αν ο κώδικας πέσει σε λούπα ή είναι πολύ βαρύς, το Gas τελειώνει, η εκτέλεση διακόπτεται ακαριαία (revert) και ο χρήστης χάνει τα χρήματα που πλήρωσε για την προσπάθεια. Αυτός ο οικονομικός μηχανισμός εξασφαλίζει την αδιάλειπτη λειτουργία του παγκόσμιου υπολογιστή.

Αυτή η υποδομή άνοιξε τις πύλες για το Web 3.0. Μέσα σε λίγα χρόνια, αρχίσαμε να βλέπουμε την ανάπτυξη Αποκεντρωμένων Εφαρμογών (Decentralized Applications - DApps), δηλαδή εφαρμογών με frontend που επικοινωνούν άμεσα με έξυπνα συμβόλαια στο backend. Η πιο ραγδαία αναπτυσσόμενη κατηγορία αυτών των εφαρμογών είναι η Αποκεντρωμένη Οικονομία (Decentralized Finance - DeFi). Στο οικοσύστημα του DeFi, παραδοσιακές τραπεζικές υπηρεσίες—όπως τα

δάνεια, η παροχή ρευστότητας και οι ανταλλαγές νομισμάτων—αντικαθίστανται από ανοιχτό κώδικα.

Ένα τέτοιο αντιπροσωπευτικό παράδειγμα λειτουργίας, όπου ο χρήστης καταθέτει ενέχυρο και δανείζεται ψηφιακά περιουσιακά στοιχεία αποκλειστικά μέσω αλγορίθμου, αναλύεται εκτενώς σε επίπεδο κώδικα (Solidity) στο Παράρτημα της παρούσας εργασίας, αποδεικνύοντας έμπρακτα την ισχύ των έξυπνων συμβολαίων έναντι των παραδοσιακών χρηματοπιστωτικών δομών.

3. Τεχνολογικό Υπόβαθρο και Βασικές Έννοιες

3.1 Τεχνολογία Blockchain: Αρχιτεκτονική και Δομή Blocks

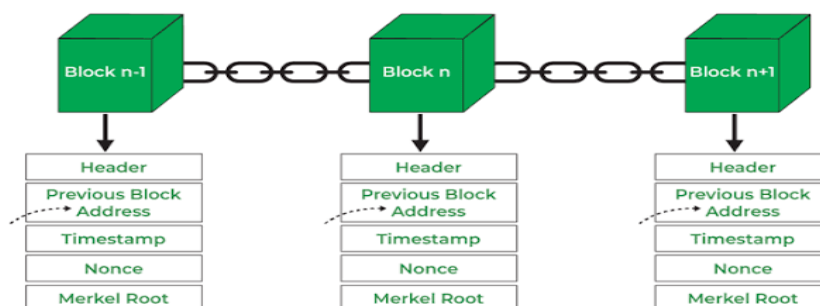
Στον πυρήνα του, το Blockchain δεν είναι τίποτα περισσότερο από μια κατανεμημένη, ψηφιακή βάση δεδομένων (distributed ledger). Η ριζική του διαφορά από τις παραδοσιακές βάσεις (όπως η SQL που χρησιμοποιείται στις τράπεζες) είναι ο τρόπος με τον οποίο οργανώνει, καταγράφει και κλειδώνει την πληροφορία. Αντί να αποθηκεύει τα δεδομένα σε απλούς πίνακες, τα ομαδοποιεί σε συγκεκριμένα "πακέτα" πληροφοριών, τα οποία ονομάζονται Blocks (μπλοκ).

Κάθε φορά που γεμίζει ένα τέτοιο μπλοκ με νέες, έγκυρες συναλλαγές, «σφραγίζεται» κρυπτογραφικά και ενώνεται οριστικά με το αμέσως προηγούμενο, σχηματίζοντας μια αδιάσπαστη γραμμική αλυσίδα. Από εκεί προκύπτει και η ονομασία "Block-chain". Για να επιτευχθεί αυτή η δομική ακεραιότητα, η αρχιτεκτονική του κάθε μπλοκ είναι αυστηρά καθορισμένη και χωρίζεται σε δύο κύρια μέρη: την Κεφαλίδα (Block Header) και το Σώμα (Block Body).

3.1.1 Η Κεφαλίδα του Μπλοκ (Block Header)

Το Header είναι ουσιαστικά ο "εγκέφαλος" του μπλοκ και αποτελεί το μοναδικό τμήμα που περνάει από τη διαδικασία του mining (εξόρυξης). Αν και το μέγεθός του είναι ελάχιστο (μόλις 80 bytes στο δίκτυο του Bitcoin), περιέχει κρίσιμα μεταδεδομένα (metadata) για την κατάσταση του δικτύου. Τα βασικότερα συστατικά του είναι:

- Το Hash του προηγούμενου μπλοκ (Previous Block Hash): Αυτό είναι το στοιχείο που δημιουργεί την "αλυσίδα". Κάθε νέο μπλοκ περιέχει στην κεφαλίδα του το ψηφιακό αποτύπωμα του μπλοκ που προηγήθηκε.
- Η Χρονosφραγίδα (Timestamp): Είναι ένας μετρητής σε μορφή Unix time που καταγράφει την ακριβή στιγμή (σε δευτερόλεπτα) που το μπλοκ βρέθηκε και προστέθηκε στο δίκτυο. Η χρονosφραγίδα εξασφαλίζει τη σωστή χρονολογική σειρά των συναλλαγών.
- Το Merkle Root (Ρίζα Merkle): Πρόκειται για ένα και μοναδικό κρυπτογραφικό hash το οποίο συμπυκνώνει μαθηματικά όλες τις συναλλαγές που περιέχονται στο σώμα του μπλοκ. Μέσω της ρίζας Merkle, η κεφαλίδα "γνωρίζει" ποια δεδομένα βρίσκονται από κάτω της, χωρίς να χρειάζεται να αποθηκεύσει ξανά όλο τον όγκο τους.
- Ο Αριθμός Nonce (Number Used Once): Είναι ένας τυχαίος αριθμός που ψάχνουν να βρουν οι miners αλλάζοντάς τον συνεχώς, με σκοπό να πετύχουν το σωστό hash που απαιτεί το δίκτυο.



Εικόνα 4: Αρχιτεκτονική δομή και διασύνδεση των Blocks σε ένα κατανεμημένο δίκτυο.

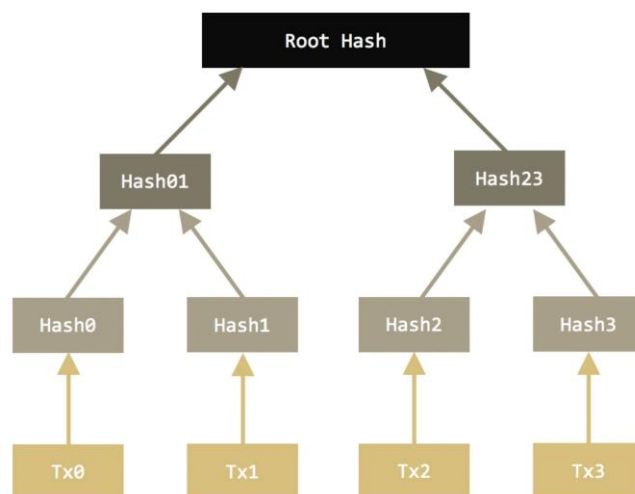
3.1.2 Το Σώμα του Μπλοκ (Block Body)

Σε αντίθεση με την κεφαλίδα, το σώμα καταλαμβάνει τον περισσότερο χώρο (στο Bitcoin φτάνει περίπου το 1 megabyte). Περιλαμβάνει την πλήρη, αναλυτική λίστα των συναλλαγών που επιβεβαιώθηκαν κατά τη διάρκεια δημιουργίας του συγκεκριμένου μπλοκ (συνήθως ένα παράθυρο 10 λεπτών). Κάθε συναλλαγή εδώ έχει τη δική της ηλεκτρονική υπογραφή και τα

3.1.3 Το Genesis Block και το Φαινόμενο της Χιονοστιβάδας

Αν ακολουθήσει κανείς την αλυσίδα προς τα πίσω, μπλοκ προς μπλοκ, διαβάζοντας τα «Previous Hashes», θα φτάσει αναπόφευκτα στην αρχή του χρόνου για το συγκεκριμένο δίκτυο. Αυτό είναι το λεγόμενο Genesis Block (Μπλοκ Γένεσης), το πρώτο μπλοκ που δημιουργήθηκε (συνήθως από τον ίδιο τον δημιουργό του πρωτοκόλλου) και το μοναδικό που, λογικά, δεν περιέχει το hash κάποιου προηγούμενου μπλοκ.

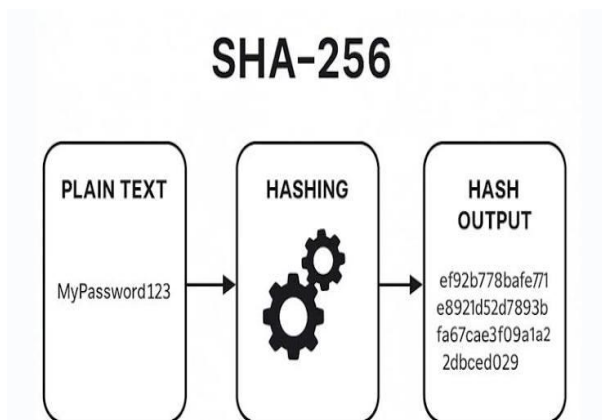
Ο τρόπος που αυτά τα κομμάτια ενώνονται δημιουργεί ένα εντυπωσιακό χαρακτηριστικό ασφαλείας. Αν κάποιος επιτιθέμενος προσπαθήσει να μπει στα αρχεία και να αλλάξει έστω και ένα γράμμα σε μια παλιά συναλλαγή, το σύστημα καταρρέει για αυτόν. Η αλλαγή στη συναλλαγή θα αλλάξει αυτόματα το Merkle Root στο Header εκείνου του μπλοκ. Αυτό, με τη σειρά του, θα αλλάξει το συνολικό hash του συγκεκριμένου μπλοκ. Το επόμενο μπλοκ στην αλυσίδα, που είχε καταγράψει το παλιό hash, θα βρεθεί να μην ταιριάζει πλέον. Το σφάλμα θα μεταδοθεί σαν χιονοστιβάδα (avalanche effect) σε όλα τα επόμενα μπλοκ, "σπάζοντας" την αλυσίδα. Οι υπόλοιποι κόμβοι του δικτύου θα δουν την ασυμφωνία, θα καταλάβουν την απάτη και θα απορρίψουν το αλλοιωμένο αρχείο ακαριαία.



Εικόνα 5: Δομή ενός Δέντρου Merkle (Merkle Tree) και ο κρυπτογραφικός κατακερματισμός των συναλλαγών.

3.2 Κρυπτογραφικές Συναρτήσεις Κατακερματισμού (Hashing) και SHA-256

Το πιο βασικό "τούβλο" στο οικοδόμημα του blockchain είναι η διαδικασία του Hashing. Με απλά λόγια, μια συνάρτηση κατακερματισμού (hash function) είναι ένας μαθηματικός αλγόριθμος. Παίρνει δεδομένα οποιουδήποτε μεγέθους —από μια απλή λέξη ή έναν κωδικό, μέχρι ολόκληρο το περιεχόμενο ενός σκληρού δίσκου— και τα μετατρέπει σε μια συμβολοσειρά σταθερού μήκους. Το αποτέλεσμα αυτής της διαδικασίας ονομάζεται ψηφιακό αποτύπωμα ή hash.



Εικόνα 6: Η λειτουργία της μονόδρομης συνάρτησης SHA-256 και το φαινόμενο της χιονοστιβάδας (Avalanche Effect).

Στην περίπτωση του Bitcoin, αλλά και πολλών άλλων κρυπτονομισμάτων, το απόλυτο πρότυπο που χρησιμοποιείται είναι ο αλγόριθμος SHA-256 (Secure Hash Algorithm 256-bit). Ο συγκεκριμένος αλγόριθμος σχεδιάστηκε από την Υπηρεσία Εθνικής Ασφαλείας των ΗΠΑ (NSA) και έχει μια πολύ συγκεκριμένη ιδιότητα: ό,τι και να του δώσεις ως είσοδο (input), αυτός θα βγάλει πάντα ένα αποτέλεσμα που αποτελείται από 256 bits, δηλαδή 64 δεκαεξαδικούς χαρακτήρες. Ούτε έναν παραπάνω, ούτε έναν λιγότερο.

Για να θεωρηθεί, ωστόσο, μια τέτοια συνάρτηση ασφαλής για χρήση σε ένα σύστημα όπως το blockchain, όπου διακυβεύονται τεράστια ποσά, πρέπει να

πληροί κάποιες πολύ αυστηρές προϋποθέσεις. Πρώτα από όλα, οφείλει να είναι απόλυτα ντετερμινιστική. Αυτό σημαίνει ότι αν περάσεις το ίδιο ακριβώς αρχείο μέσα από τον αλγόριθμο χίλιες φορές, θα πάρεις χίλιες φορές το ίδιο ακριβώς hash. Αν όμως ανοίξεις το αρχείο και αλλάξεις έστω και ένα κόμμα, ή προσθέσεις ένα κενό, το τελικό ψηφιακό αποτύπωμα θα αλλάξει ριζικά και απρόβλεπτα. Στην κρυπτογραφία αυτό είναι γνωστό ως «φαινόμενο της χιονοστιβάδας» (avalanche effect). Είναι το χαρακτηριστικό που μας επιτρέπει να ελέγχουμε ακαριαία αν κάποιος πείραξε τα δεδομένα μιας συναλλαγής. Αν έστω και ένα ψηφίο αλλάξει, το hash της συναλλαγής αλλάζει τελείως, χτυπώντας "συναγερμό" στο δίκτυο.

Ένα άλλο κρίσιμο στοιχείο είναι η μονόδρομη λειτουργία της (one-way function). Μπορείς πανεύκολα και σε κλάσματα δευτερολέπτου να υπολογίσεις το hash από ένα οποιοδήποτε αρχείο. Είναι όμως υπολογιστικά αδύνατο να κάνεις το ανάποδο. Δεν υπάρχει μαθηματικός τύπος που να παίρνει το hash και να σου αποκαλύπτει ποιο ήταν το αρχικό αρχείο. Ο μόνος τρόπος να το βρεις είναι να δοκιμάζεις στα τυφλά (brute-force) διαφορετικά inputs, μέχρι το hash που θα παραχθεί να ταιριάζει με αυτό που ψάχνεις. Αυτή ακριβώς η εξαντλητική δοκιμή τυχαίων αριθμών είναι αυτό που κάνουν οι υπολογιστές των miners στο δίκτυο, καταναλώνοντας τεράστια ποσά ενέργειας.

Τέλος, η συνάρτηση πρέπει να αντέχει στις λεγόμενες συγκρούσεις (collision resistance). Σύγκρουση προκύπτει όταν δύο διαφορετικά αρχεία βγάλουν, εντελώς συμπτωματικά, το ίδιο hash. Θεωρητικά, επειδή τα πιθανά inputs είναι άπειρα αλλά τα πιθανά hashes είναι πεπερασμένα (έστω και αν πρόκειται για τον ασύλληπτα μεγάλο αριθμό του), είναι μαθηματικά βέβαιο ότι κάποιες συγκρούσεις υπάρχουν. Στην πράξη, όμως, ο αριθμός των πιθανών συνδυασμών του SHA-256 είναι μεγαλύτερος από το πλήθος των ατόμων στο ορατό σύμπαν. Συνεπώς, η πιθανότητα να βρει κάποιος μια σύγκρουση θεωρείται μηδενική με τα σημερινά δεδομένα της υπολογιστικής ισχύος. Έτσι, το blockchain μπορεί να βασίζεται στα hashes ως τη μοναδική, απαραβίαστη και αμετάβλητη ταυτότητα της κάθε συναλλαγής.

3.3 Μηχανισμοί Συναίνεσης (Consensus Mechanisms)

Η απουσία μιας κεντρικής αρχής στο Blockchain καθιστά αναγκαία την ύπαρξη ενός πρωτοκόλλου που επιτρέπει στους κατανεμημένους κόμβους να καταλήξουν σε συμφωνία (consensus) σχετικά με την τρέχουσα κατάσταση του καθολικού. Σε μια συμβατική, σχεσιακή βάση δεδομένων (όπως αυτές που χρησιμοποιούν οι τράπεζες), αν προκύψει οποιαδήποτε διαφωνία για το υπόλοιπο ενός λογαριασμού, ο κεντρικός διαχειριστής του συστήματος (system administrator) έχει τον τελευταίο λόγο και επιβάλλει την "αλήθεια". Στο οικοσύστημα του blockchain, ωστόσο, όλοι οι κόμβοι είναι απολύτως ισότιμοι. Επομένως, το τεχνικό ερώτημα δεν είναι απλώς πώς μεταδίδονται τα δεδομένα από υπολογιστή σε υπολογιστή, αλλά πώς χιλιάδες άγνωστοι μεταξύ τους συμμετέχοντες αποφασίζουν συλλογικά ποια εκδοχή της αλήθειας είναι η σωστή, ειδικά όταν κάποιοι από αυτούς έχουν οικονομικό κίνητρο να εξαπατήσουν το σύστημα.

Οι μηχανισμοί αυτοί διασφαλίζουν ουσιαστικά ότι το δίκτυο παραμένει ανθεκτικό σε επιθέσεις και οργανωμένες προσπάθειες αλλοίωσης των δεδομένων. Για να επιτευχθεί αυτό, τα πρωτόκολλα συναίνεσης επιβάλλουν ένα "κόστος συμμετοχής". Μεταφράζουν, δηλαδή, είτε την υπολογιστική είτε την οικονομική ισχύ ενός χρήστη σε δικαίωμα ψήφου, αποτρέποντας την ανεξέλεγκτη δημιουργία ψεύτικων λογαριασμών (Sybil Attacks).

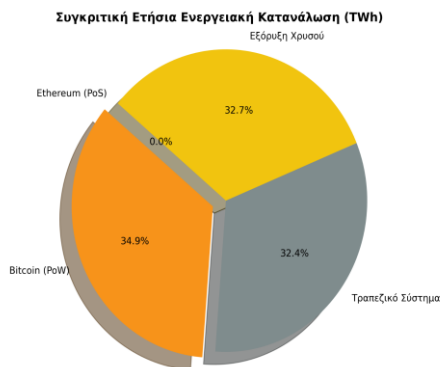
3.3.1 Απόδειξη Εργασίας (Proof of Work - PoW)

Ο μηχανισμός Proof of Work, ο οποίος εισήχθη για πρώτη φορά από το δίκτυο του Bitcoin, βασίζεται στην επίλυση ενός εξαιρετικά δύσκολου υπολογιστικού προβλήματος. Στην πράξη, η διαδικασία αυτή προσομοιάζει με έναν αδυσώπητο, παγκόσμιο μαθηματικό διαγωνισμό. Οι "εξορύκτες" (miners) του δικτύου ανταγωνίζονται σκληρά μεταξύ τους για να βρουν πρώτοι έναν συγκεκριμένο τυχαίο αριθμό, ο οποίος ονομάζεται Nonce (Number Used Once).

Είναι σημαντικό να τονιστεί ότι δεν υπάρχει κάποιος έξυπνος αλγόριθμος ή μαθηματική συντόμευση για να βρει κανείς το Nonce. Ο μόνος τρόπος είναι η εξαντλητική δοκιμή (brute-forcing). Τα μηχανήματα δοκιμάζουν δισεκατομμύρια αριθμούς κάθε δευτερόλεπτο. Ο τελικός στόχος είναι ο συνδυασμός των δεδομένων του νέου block μαζί με το Nonce να παράγει ένα κρυπτογραφικό hash που ικανοποιεί μια αυστηρή συνθήκη (το λεγόμενο target difficulty) που έχει

θέσει το ίδιο το δίκτυο. Όταν το hash βρεθεί, το block θεωρείται έγκυρο, προστίθεται στην αλυσίδα και ο εξορύκτης κερδίζει τη δυνατότητα να καταγράψει τις συναλλαγές, λαμβάνοντας ως ανταμοιβή τα αντίστοιχα κρυπτονομίσματα.

Το κύριο πλεονέκτημα του PoW είναι η εξαιρετικά υψηλή ασφάλεια που προσφέρει. Η ασφάλεια αυτή είναι πρακτικά "θερμοδυναμική". Για να μπορέσει ένας επιτιθέμενος να ακυρώσει ή να αντιστρέψει μια συναλλαγή στο δίκτυο του Bitcoin, θα έπρεπε να συγκεντρώσει περισσότερη υπολογιστική ισχύ από αυτήν που διαθέτει το υπόλοιπο δίκτυο αθροιστικά (Επίθεση 51%). Ωστόσο, η ακαδημαϊκή βιβλιογραφία επισημαίνει σταθερά ως κύριο μειονέκτημα την τεράστια κατανάλωση ηλεκτρικής ενέργειας. Εκατομμύρια μηχανήματα παγκοσμίως εκτελούν ταυτόχρονα τις ίδιες "άχρηστες" μαθηματικές πράξεις, δαπανώντας ενέργεια που συχνά ξεπερνά την ετήσια κατανάλωση ολόκληρων κρατών.



Εικόνα 7: Συγκριτική κατανομή της ετήσιας ενεργειακής κατανάλωσης (σε TWh) μεταξύ αποκεντρωμένων δικτύων, εξόρυξης χρυσού και παραδοσιακού τραπεζικού συστήματος

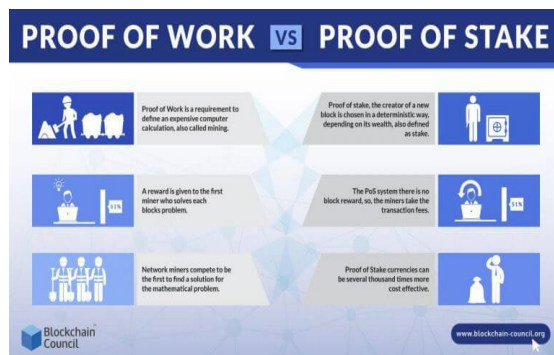
αντιληφθεί ότι ένας επικυρωτής επιχειρεί να εγκρίνει διπλές ή ψευδείς συναλλαγές, ενεργοποιείται αυτόματα ένας αλγόριθμος ποινής (slashing), ο οποίος καταστρέφει ένα μέρος ή και το σύνολο των κλειδωμένων χρημάτων του. Η προσέγγιση αυτή αλλάζει τους κανόνες του παιχνιδιού. Μειώνει την ενεργειακή κατανάλωση κατά 99.9%, όπως ακριβώς συνέβη με την ιστορική μετάβαση του δικτύου Ethereum στο PoS (το γνωστό ως "The Merge").

Πέρα από το περιβαλλοντικό όφελος, το PoS επιτρέπει μεγαλύτερη ταχύτητα στις συναλλαγές, καθώς απαλλάσσει το δίκτυο από τη χρονοβόρα διαδικασία της επίλυσης κρυπτογραφικών γρίφων. Παρ' όλα αυτά, το μοντέλο εγείρει σοβαρές συζητήσεις στην κοινότητα σχετικά με την πιθανή συγκέντρωση ισχύος. Πολλοί ερευνητές υποστηρίζουν ότι το σύστημα ευνοεί όσους κατέχουν ήδη τα περισσότερα κεφάλαια, δημιουργώντας συνθήκες "πλουτοκρατίας", αφού όσο περισσότερα νομίσματα δεσμεύει κάποιος, τόσο συχνότερα επιλέγεται για να επικυρώσει blocks και να κερδίσει νέες ανταμοιβές.

3.3.2 Απόδειξη Συμμετοχής (Proof of Stake - PoS)

Ως εναλλακτική λύση στο τεράστιο πρόβλημα της ενέργειας, η κοινότητα ανέπτυξε τον μηχανισμό Proof of Stake. Εδώ, το σύστημα δεν απαιτεί πλέον υπολογιστική ισχύ. Η επιλογή του κόμβου που θα αποκτήσει το δικαίωμα να δημιουργήσει το επόμενο block δεν εξαρτάται από τον εξοπλισμό του (hardware), αλλά άμεσα από το ποσοστό των νομισμάτων (stake) που κατέχει και δεσμεύει ως εγγύηση στο δίκτυο.

Σε αυτό το περιβάλλον, οι "επικυρωτές" (validators) αντικαθιστούν πλήρως τον ρόλο που είχαν οι miners. Αντί να σπαταλούν ηλεκτρικό ρεύμα, οι επικυρωτές «κλειδώνουν» το δικό τους κεφάλαιο μέσα σε ένα έξυπνο συμβόλαιο. Αν το πρωτόκολλο



Εικόνα 8: Συγκριτική αναπαράσταση λειτουργίας των μηχανισμών Απόδειξης Εργασίας (PoW) και Απόδειξης Συμμετοχής (PoS).

3.4 Ψηφιακά Tokens και Έξυπνα Συμβόλαια (Smart Contracts)

Η εξέλιξη της τεχνολογίας Blockchain από την πρώτη γενιά (Bitcoin) στη δεύτερη γενιά, οδήγησε στη δημιουργία πλήρως προγραμματιζόμενων δικτύων, με τον αδιαμφισβήτητο ηγέτη σε αυτόν τον τομέα να είναι το Ethereum. Η μεγάλη καινοτομία σε αυτή τη φάση δεν ήταν απλώς η μεταφορά ψηφιακού χρήματος από τον χρήστη Α στον χρήστη Β. Η πραγματική επανάσταση ήταν η ικανότητα αποθήκευσης και εκτέλεσης αυτόνομου κώδικα απευθείας πάνω στην αλυσίδα των blocks. Το δίκτυο μετατράπηκε ουσιαστικά σε έναν παγκόσμιο αποκεντρωμένο υπολογιστή.

3.4.1 Έξυπνα Συμβόλαια (Smart Contracts)

Στον πυρήνα αυτού του παγκόσμιου υπολογιστή βρίσκονται τα Έξυπνα Συμβόλαια (Smart Contracts). Ο όρος μπορεί να ακούγεται νομικός, αλλά στην πραγματικότητα πρόκειται για καθαρά υπολογιστικά αυτοεκτελούμενα προγράμματα (backend scripts) τα οποία μεταφράζουν τους όρους μιας οποιασδήποτε συμφωνίας απευθείας σε γραμμές κώδικα.

Ο Nick Szabo, ο επιστήμονας υπολογιστών που επινόησε τον όρο πολύ πριν υπάρξει το blockchain, τα είχε παρομοιάσει με έναν αυτόματο πωλητή αναψυκτικών. Η λογική είναι καθαρά ντετερμινιστική, βασισμένη στο μοντέλο «αν συμβεί αυτό, τότε εκτέλεσε εκείνο» (if-this-then-that). Αν ρίξεις το σωστό κέρμα (συνθήκη) και πατήσεις το κουμπί, το μηχάνημα θα σου δώσει το αναψυκτικό (αποτέλεσμα). Μόλις ικανοποιηθούν οι προκαθορισμένες συνθήκες στον κώδικα, το συμβόλαιο εκτελείται αυτόματα, κλειδώνοντας την απόφαση χωρίς την ανάγκη κανενός ενδιαμέσου μεσάζοντα, δικηγόρου ή τραπεζικού υπαλλήλου.

Το πιο καθοριστικό χαρακτηριστικό τους, ωστόσο, είναι το γεγονός ότι είναι απολύτως αμετάβλητα (immutable). Από τη στιγμή που ένας προγραμματιστής κάνει deploy (μεταφόρτωση) τον κώδικα ενός έξυπνου συμβολαίου στο δίκτυο, το πρόγραμμα αυτό παγιώνεται. Δεν μπορεί να διαγραφεί, να τροποποιηθεί ή να αλλοιωθεί από κανέναν — ούτε καν από τον ίδιο τον δημιουργό του. Αυτό από τη μία πλευρά εγγυάται τη διαφάνεια, καθώς όλοι γνωρίζουν ότι το συμβόλαιο θα κάνει ακριβώς αυτό που έχει προγραμματιστεί να κάνει. Από την άλλη πλευρά, απαιτεί τέλειο προγραμματισμό (όπως φαίνεται και στον κώδικα Solidity που παρατίθεται στο Παράρτημα της εργασίας), διότι αν υπάρξει κάποιο κενό ασφαλείας (bug) στον κώδικα, οι hackers μπορούν να το εκμεταλλευτούν χωρίς να μπορεί κανείς να σταματήσει την εκτέλεσή του.

3.4.2 Ψηφιακά Tokens και Πρότυπα

Συχνά, ο κόσμος μπερδεύει τα κρυπτονομίσματα (coins) με τα tokens. Για να το ξεκαθαρίσουμε τεχνικά, ένα κρυπτονόμισμα (όπως το ETH) είναι το εγγενές νόμισμα του ίδιου του blockchain. Αντίθετα, ένα token δεν έχει δικό του δίκτυο. Δημιουργείται, ζει και μεταφέρεται αποκλειστικά μέσω ενός έξυπνου συμβολαίου που τρέχει πάνω σε ένα ήδη υπάρχον δίκτυο. Ουσιαστικά, ένα token είναι απλώς μια μεταβλητή σε μια βάση δεδομένων ενός smart contract, το οποίο κρατάει αρχείο με το ποιες διευθύνσεις κατέχουν ποιο υπόλοιπο.

Για να μπορούν τα ανταλλακτήρια και τα ψηφιακά πορτοφόλια να συνεργάζονται απρόσκοπτα με αυτά τα συμβόλαια, η κοινότητα δημιούργησε συγκεκριμένα πρότυπα προγραμματισμού. Ανάλογα με τη χρήση τους, τα ψηφιακά tokens χωρίζονται σε δύο κυρίαρχες κατηγορίες:

A) Fungible Tokens (Ανταλλάξιμα – Πρότυπο ERC-20) Ο όρος "εναλλαξιμότητα" (fungibility) αναφέρεται σε αγαθά που είναι πανομοιότυπα και μπορούν να αντικατασταθούν το ένα από το άλλο. Για παράδειγμα, ένα χαρτονόμισμα των 10 ευρώ έχει ακριβώς την ίδια αξία και χρηστικότητα με ένα οποιοδήποτε άλλο χαρτονόμισμα των 10 ευρώ. Στο blockchain του Ethereum, το πρότυπο για τέτοια tokens ονομάζεται ERC-20. Κάθε μονάδα ενός ERC-20 token είναι απολύτως ίση με μια άλλη. Σε αυτή την κατηγορία ανήκουν τα περισσότερα ψηφιακά περιουσιακά στοιχεία, όπως τα νομίσματα διακυβέρνησης (governance tokens) διάφορων εφαρμογών, καθώς και τα περίφημα Stablecoins (π.χ. USDT, USDC) τα οποία έχουν την αξία τους "κλειδωμένη" σε ισοτιμία ένα προς ένα με το αμερικανικό δολάριο.

B) Non-Fungible Tokens - NFTs (Μη Ανταλλάξιμα – Πρότυπο ERC-721) Στον αντίποδα, υπάρχουν περιπτώσεις όπου χρειαζόμαστε ψηφιακή μοναδικότητα (digital scarcity). Τα NFTs είναι μοναδικά ψηφιακά στοιχεία που δεν μπορούν να αντικατασταθούν ή να κοπούν σε μικρότερα

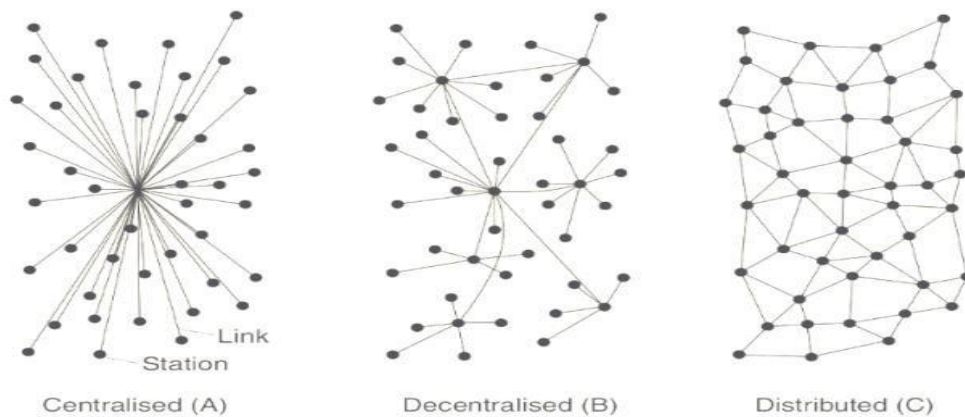
κομμάτια. Φανταστείτε τον πίνακα της Μόνα Λίζα: δεν μπορείς να τον ανταλλάξεις με μια απλή αφίσα του, ούτε μπορείς να τον κόψεις στη μέση. Βασισμένα κυρίως στο πρότυπο ERC-721, τα NFTs εισήγαγαν για πρώτη φορά την έννοια της κρυπτογραφικής ιδιοκτησίας. Ενώ έγιναν ευρέως γνωστά μέσω της ψηφιακής τέχνης και των συλλογών, η πραγματική τους τεχνολογική αξία βρίσκεται αλλού: χρησιμοποιούνται πλέον για την πιστοποίηση κυριότητας πραγματικών ακινήτων (Real World Assets tokenization), για ψηφιακές ταυτότητες (digital identity), διπλώματα ευρεσιτεχνίας, μέχρι και για ιχνηλασιμότητα προϊόντων στην εφοδιαστική αλυσίδα.

4. Ανάλυση Εφαρμογών και Κοινωνικοοικονομική Επίδραση

4.1 Παρουσίαση Online Εφαρμογών και Πλατφορμών

Τα ανταλλακτήρια αποτελούν την κύρια πύλη εισόδου (on-ramp) των χρηστών στο οικοσύστημα των ψηφιακών νομισμάτων. Λειτουργούν ως αγορές όπου ανταλλάσσονται κρυπτονομίσματα με παραδοσιακά (fiat) νομίσματα ή με άλλα ψηφιακά περιουσιακά στοιχεία. Τεχνολογικά και λειτουργικά, χωρίζονται σε δύο κύριες κατηγορίες:

- Κεντριοποιημένα Ανταλλακτήρια (Centralized Exchanges - CEXs): Πλατφόρμες όπως η Binance και η Coinbase λειτουργούν με παρόμοιο τρόπο με τα παραδοσιακά χρηματιστήρια. Η αρχιτεκτονική τους βασίζεται σε κεντρικούς διακομιστές (backend servers) και παραδοσιακές σχεσιακές βάσεις δεδομένων που διαχειρίζονται ένα Βιβλίο Εντολών (Order Book). Το CEX λειτουργεί ως θεματοφύλακας (custodian), διατηρώντας τα ιδιωτικά κλειδιά (private keys) των χρηστών στα δικά του πορτοφόλια. Αν και προσφέρουν υψηλή ρευστότητα (liquidity) και ταχύτητα εκτέλεσης συναλλαγών χάρη στην off-chain (εκτός αλυσίδας) λειτουργία τους, αποτελούν "μοναδικά σημεία αποτυχίας" (single points of failure) και υπόκεινται στον κίνδυνο κυβερνοεπιθέσεων.
- Αποκεντρωμένα Ανταλλακτήρια (Decentralized Exchanges - DEXs): Πλατφόρμες όπως το Uniswap αποτελούν μια καινοτομία της κατανεμημένης αρχιτεκτονικής. Σε ένα DEX, δεν υπάρχει κεντρικός διακομιστής ούτε Order Book. Αντιθέτως, η λογική ανταλλαγής (trade logic) είναι κωδικοποιημένη σε αυτοεκτελούμενα Έξυπνα Συμβόλαια (Smart Contracts). Οι χρήστες διατηρούν τον πλήρη έλεγχο των ιδιωτικών τους κλειδιών (non-custodial) και οι συναλλαγές γίνονται απευθείας (peer-to-peer) on-chain. Η λειτουργία τους βασίζεται στους Αυτοματοποιημένους Ειδικούς Διαπραγματευτές (Automated Market Makers - AMMs), όπου η τιμή των περιουσιακών στοιχείων καθορίζεται αλγοριθμικά, συνήθως μέσω της μαθηματικής φόρμουλας σταθερού γινομένου ($x * y = k$), βάσει της διαθέσιμης ρευστότητας στις δεξαμενές (liquidity pools).



Εικόνα 9: Τοπολογική σύγκριση Κεντριοποιημένων και Κατανεμημένων συστημάτων δικτύου

4.2 Πρωτόκολλα Αποκεντρωμένης Οικονομίας (Decentralized Finance - DeFi)

Ο όρος DeFi αναφέρεται σε ένα σύνολο χρηματοοικονομικών υπηρεσιών (δανεισμός, ασφάλιση, αποταμίευση, παραγωγή αποδόσεων) που κατασκευάζονται αποκλειστικά πάνω σε δημόσια δίκτυα blockchain (κυρίως στο Ethereum). Αφαιρώντας τους μεσάζοντες, όπως τις εμπορικές τράπεζες, το DeFi αξιοποιεί τον κώδικα για να αυτοματοποιήσει την εμπιστοσύνη. Μια από τις πιο διαδεδομένες εφαρμογές είναι τα πρωτόκολλα δανεισμού (Lending and Borrowing Protocols), όπως το Aave και το Compound. Σε αυτά τα συστήματα, η διαδικασία δανεισμού δεν βασίζεται στην πιστοληπτική ικανότητα του χρήστη (credit score), καθώς το σύστημα είναι ψευδώνυμο. Αντιθέτως, χρησιμοποιείται η αρχή της "υπερ-εξασφάλισης" (over-collateralization). Ο χρήστης οφείλει να κλειδώσει σε ένα έξυπνο συμβόλαιο κρυπτονομίσματα μεγαλύτερης αξίας από αυτά

που επιθυμεί να δανειστεί. Εάν η αξία του ενεχύρου πέσει κάτω από ένα προκαθορισμένο αλγοριθμικό όριο, το έξυπνο συμβόλαιο εκτελεί αυτόματα ρευστοποίηση (liquidation) για να προστατεύσει τους καταθέτες (liquidity providers), διασφαλίζοντας την οικονομική ακεραιότητα του πρωτοκόλλου εξ ολοκλήρου μέσω κώδικα.

4.3 Κοινωνικές Επιπτώσεις και Ζητήματα Ασφάλειας

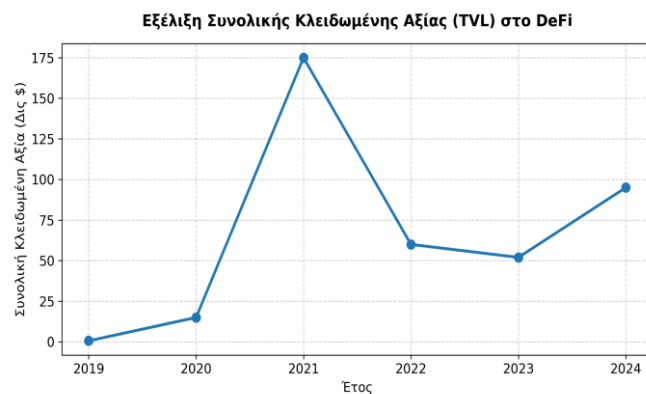
Η ραγδαία εξέλιξη και υιοθέτηση των τεχνολογιών Blockchain δεν περιορίζεται μόνο στη δημιουργία νέων χρηματοοικονομικών εργαλείων, αλλά επιφέρει βαθιές κοινωνικές αλλαγές. Μέχρι σήμερα, η κοινωνία μας ήταν δομημένη γύρω από την έννοια της "θεσμικής εμπιστοσύνης". Έπρεπε να εμπιστευτούμε τράπεζες, κυβερνήσεις και δικηγόρους για να επιβεβαιώσουν ποιος κατέχει τι. Παράλληλα, όμως, η αποκεντρωμένη φύση του οικοσυστήματος εισάγει πρωτοφανείς προκλήσεις στον τομέα της κυβερνοασφάλειας, μεταφέροντας την ευθύνη προστασίας από τους κεντρικούς φορείς στον ίδιο τον τελικό χρήστη. Αυτή η μετάβαση από το παραδοσιακό μοντέλο στο Web3 κρύβει τεράστιες ευκαιρίες, αλλά και θανάσιμες παγίδες για τους μη εξοικειωμένους.

4.3.1 Χρηματοοικονομική Συμπερίληψη και Εκδημοκρατισμός

Μία από τις σημαντικότερες κοινωνικές επιδράσεις των κρυπτονομισμάτων είναι η δυνατότητα χρηματοοικονομικής συμπερίληψης (financial inclusion). Σύμφωνα με επίσημα δεδομένα από την Παγκόσμια Τράπεζα, ένα μεγάλο ποσοστό του παγκόσμιου πληθυσμού παραμένει "unbanked", δηλαδή στερείται πλήρως την πρόσβαση σε βασικές τραπεζικές υπηρεσίες, κυρίως σε αναπτυσσόμενες χώρες. Οι άνθρωποι αυτοί δεν μπορούν να πάρουν δάνειο, δεν μπορούν να αποταμιεύσουν με ασφάλεια και πληρώνουν υπέρογκες προμήθειες σε εταιρείες εμβασμάτων για να λάβουν χρήματα από συγγενείς τους στο εξωτερικό.

Το οικοσύστημα των κρυπτονομισμάτων καταργεί οριστικά τα γεωγραφικά και γραφειοκρατικά εμπόδια. Δεν ζητάει πιστοποιητικά γέννησης, εκκαθαριστικά εφορίας ή ιστορικό πιστοληπτικής ικανότητας (credit score). Οποιοσδήποτε διαθέτει μια απλή σύνδεση στο διαδίκτυο και ένα έξυπνο κινητό τηλέφωνο μπορεί να δημιουργήσει ένα ψηφιακό πορτοφόλι σε δευτερόλεπτα, αποκτώντας άμεσα τη δυνατότητα να αποθηκεύει αξία και να πραγματοποιεί διασυνοριακές συναλλαγές (cross-border payments) με ελάχιστο κόστος και χωρίς την έγκριση κανενός κεντρικού ιδρύματος.

Επιπλέον, σε χώρες που μαστίζονται από ακραίο πληθωρισμό (όπως η Αργεντινή ή η Βενεζουέλα), τα αποκεντρωμένα νομίσματα —και ιδιαίτερα τα stablecoins που συνδέονται με το δολάριο— λειτουργούν ως σανίδα σωτηρίας για την προστασία της αγοραστικής δύναμης των πολιτών. Αυτή η «άδεια χωρίς σύνορα» λειτουργία εκδημοκρατίζει επί της ουσίας την πρόσβαση στο παγκόσμιο εμπόριο, δίνοντας τα ίδια ακριβώς ψηφιακά εργαλεία σε έναν αγρότη στην Αφρική και σε έναν επενδυτή στη Wall Street.



Εικόνα 10: Εξέλιξη της Συνολικής Κλειδωμένης Αξίας (Total Value Locked - TVL) στα πρωτόκολλα της Αποκεντρωμένης Οικονομίας (DeFi) για την περίοδο 2019-2024.

4.3.2 Ιδιωτικότητα vs. Κανονιστική Συμμόρφωση

Ένα εξίσου κρίσιμο κοινωνικό και νομικό ζήτημα που απασχολεί έντονα τους νομοθέτες, είναι η λεπτή ισορροπία μεταξύ της προστασίας της ιδιωτικότητας των πολιτών και της αποτροπής εγκληματικών δραστηριοτήτων. Υπάρχει μια γενικευμένη παρανόηση ότι τα κρυπτονομίσματα προσφέρουν απόλυτη ανωνυμία. Στην πραγματικότητα, τα περισσότερα δημόσια blockchains, όπως το Bitcoin, δεν είναι ανώνυμα αλλά ψευδώνυμα (pseudonymous).

Τι ακριβώς σημαίνει αυτό; Ενώ τα πραγματικά ονόματα των χρηστών (π.χ. "Γιάννης") δεν καταγράφονται πουθενά, όλες οι συναλλαγές είναι δημόσια διαθέσιμες και ορατές στο καθολικό,

σθενά συνδεδεμένες με τις αντίστοιχες κρυπτογραφικές διευθύνσεις (public keys). Στα πρώτα χρόνια του δικτύου, αυτή η ψευδωνυμία αξιοποιήθηκε πράγματι από παράνομα δίκτυα στο Dark Web (όπως το διαβόητο Silk Road) για την αγοραπωλησία παράνομων αγαθών και το ξέπλυμα χρήματος.

Σήμερα, ωστόσο, η πραγματικότητα είναι πολύ διαφορετική. Η επιστήμη της ανάλυσης αλυσίδας (chain analysis) έχει εξελιχθεί σε τέτοιο βαθμό που ειδικευμένες εταιρείες και οι διωκτικές αρχές μπορούν να ιχνηλατήσουν ροές κεφαλαίων πολύ πιο γρήγορα και αποτελεσματικά από ό,τι στο παραδοσιακό, δαιδαλώδες τραπεζικό σύστημα. Αν μια διεύθυνση συνδεθεί έστω και μία φορά με μια πραγματική ταυτότητα (π.χ. σε μια ανάληψη από ανταλλακτήριο), όλο το ιστορικό του χρήστη αποκαλύπτεται. Αυτό το γεγονός δημιουργεί διαρκείς πιέσεις από τις κυβερνήσεις για αυστηρότερη κανονιστική συμμόρφωση. Πλέον, διεθνή πλαίσια, όπως ο κανονισμός MiCA (Markets in Crypto-Assets) της Ευρωπαϊκής Ένωσης, επιβάλλουν αυστηρές διαδικασίες "Γνώριζε τον Πελάτη σου" (Know Your Customer - KYC) και "Καταπολέμηση Νομιμοποίησης Εσόδων" (Anti-Money Laundering - AML), τις οποίες τα κεντρικοποιημένα ανταλλακτήρια είναι πλέον υποχρεωμένα να εφαρμόζουν σε κάθε νέο χρήστη.

4.3.3 Τεχνολογικές Ευπάθειες και Κίνδυνοι Ασφάλειας

Στο αμιγώς τεχνικό πεδίο, η μετατόπιση της εμπιστοσύνης από τους ανθρώπους στον κώδικα σημαίνει ότι τα σφάλματα λογισμικού μπορούν να έχουν καταστροφικές οικονομικές συνέπειες. Χωρίς κεντρική αρχή, δεν υπάρχει τράπεζα για να ακυρώσει μια κακόβουλη συναλλαγή. Τα κυριότερα ζητήματα ασφάλειας αφορούν:

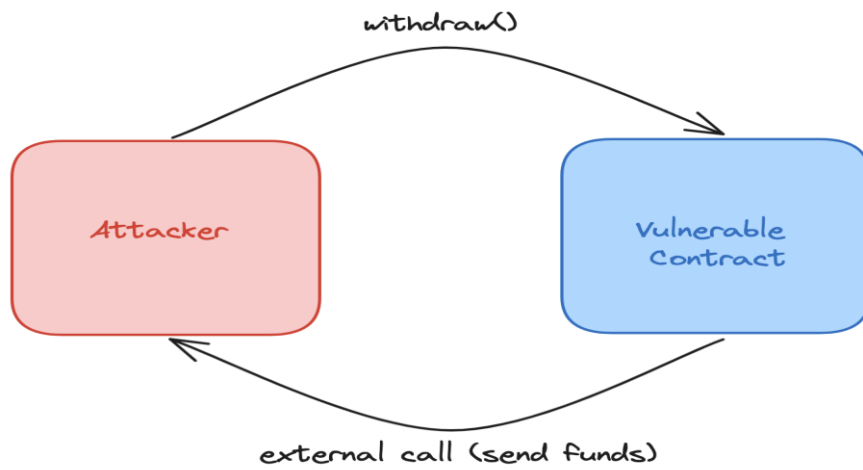
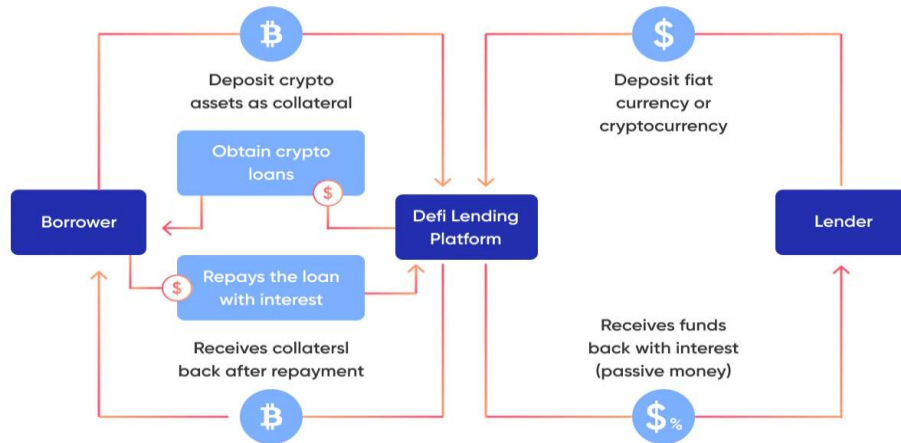
Α) Ευπάθειες Έξυπνων Συμβολαίων (Smart Contract Vulnerabilities): Δεδομένου ότι τα έξυπνα συμβόλαια είναι αμετάβλητα (immutable) μετά την ανάπτυξή τους (deployment) στο δημόσιο δίκτυο, τυχόν λογικά σφάλματα (bugs) στον κώδικα δεν μπορούν να διορθωθούν εύκολα με ένα απλό "update". Το πιο χαρακτηριστικό παράδειγμα κρίσιμης ευπάθειας είναι η επίθεση επανεισόδου (Reentrancy Attack). Σε αυτή την περίπτωση, ένας κακόβουλος χρήστης εκμεταλλεύεται τη σειρά εκτέλεσης των εντολών ενός συμβολαίου για να αντλήσει επανειλημμένα κεφάλαια, προτού το συμβόλαιο προλάβει να ενημερώσει το λογιστικό υπόλοιπο (balance) του χρήστη στο σύστημα. Τέτοιες ευπάθειες έχουν οδηγήσει στο παρελθόν σε δραματικές απώλειες εκατοντάδων εκατομμυρίων δολαρίων στο οικοσύστημα του DeFi.

*Σημείωση: Ακριβώς για την αποτροπή τέτοιων καταστροφικών επιθέσεων, στην υλοποίηση του Αποκεντρωμένου Πρωτοκόλλου Δανεισμού που παρατίθεται στο Παράρτημα Α της παρούσας εργασίας, έχει γίνει ρητή χρήση του ελεγκτή (modifier) **nonReentrant**. Ο μηχανισμός αυτός «κλειδώνει» την κατάσταση του συμβολαίου κατά τη διάρκεια μιας συνδιαλλαγής, διασφαλίζοντας την ακεραιότητα των κεφαλαίων πριν την ολοκλήρωση οποιασδήποτε εξωτερικής κλήσης.*

Β) Επιθέσεις 51% (51% Attacks): Σε δίκτυα που χρησιμοποιούν τον αλγόριθμο Proof of Work, εάν μια μεμονωμένη οντότητα ή ένα οργανωμένο pool καταφέρει να ελέγξει πάνω από το 50% της συνολικής υπολογιστικής ισχύος (hash rate) του δικτύου, αποκτά τη δυνατότητα να αναδιατάξει τα blocks. Αυτό επιτρέπει τη διαγραφή πρόσφατων συναλλαγών και τη «διπλή δαπάνη» (double-spending) των ίδιων νομισμάτων. Ενώ κάτι τέτοιο θεωρείται πρακτικά αδύνατο και ασύμφορο σε τεράστια δίκτυα με κολοσσιαία ισχύ, όπως το Bitcoin, μικρότερα blockchains έχουν πέσει επανειλημμένα θύματα τέτοιων επιθέσεων, χάνοντας την εμπιστοσύνη του κοινού.

Γ) Διαχείριση Ιδιωτικών Κλειδιών (Self-Custody Risks): Ίσως η πιο υποτιμημένη πρόκληση για τον μέσο χρήστη είναι η αυτο-φύλαξη (self-custody). Η απουσία κεντρικής υποστήριξης σημαίνει πρακτικά ότι δεν υπάρχει απουσία κουμπιού "ανάκτηση κωδικού πρόσβασης" ούτε τμήμα εξυπηρέτησης πελατών. Αυτό καθιστά τον χρήστη αποκλειστικά υπεύθυνο για την ασφάλεια των κεφαλαίων του. Η απώλεια της φράσης ανάκτησης (seed phrase) ή η πώληση θύματος επιθέσεων "ψαρέματος" (social engineering / phishing) συνεπάγεται την οριστική, μη αναστρέψιμη απώλεια των ψηφιακών περιουσιακών στοιχείων. Δεν υπάρχει κανένας οργανισμός εγγύησης καταθέσεων για να αποζημιώσει τα θύματα, γεγονός που αποτελεί, μέχρι και σήμερα, ένα από τα μεγαλύτερα εμπόδια για τη μαζική υιοθέτηση (mass adoption) της τεχνολογίας από το ευρύ κοινό.

4IRE HOW DO DEFI LOANS WORK



5. Προηγμένες Κρυπτογραφικές Υποδομές και Ασφάλεια Δικτύων

Η θεμελιώδης διαφορά των αποκεντρωμένων δικτύων σε σχέση με τα συμβατικά πληροφοριακά συστήματα, έγκειται στο μοντέλο εμπιστοσύνης. Στα συμβατικά δίκτυα, η ασφάλεια βασίζεται στο μοντέλο της "περιμετρικής άμυνας" (μέσω firewalls και συστημάτων ανίχνευσης εισβολών) και της κεντρικής διαχείρισης ταυτοτήτων. Αντιθέτως, στα δίκτυα Blockchain, όπου το περιβάλλον είναι εξ ορισμού εχθρικό (adversarial) και οι κόμβοι λειτουργούν αυτόνομα και ανώνυμα, το μοντέλο αυτό καταρρέει πλήρως. Τον ρόλο του εγγυητή της αλήθειας αναλαμβάνουν αποκλειστικά τα ανώτερα μαθηματικά και, πιο συγκεκριμένα, η κρυπτογραφία.

5.1 Ο Ρόλος της Κρυπτογραφίας σε Περιβάλλοντα Μηδενικής Εμπιστοσύνης (Trustless Environments)

Η θεμελιώδης αρχιτεκτονική του Blockchain βασίζεται στην έννοια του περιβάλλοντος "μηδενικής εμπιστοσύνης" (trustless environment). Ο όρος αυτός δεν υποδηλώνει την απουσία εμπιστοσύνης, αλλά τη ριζική μετατόπισή της: οι χρήστες δεν χρειάζεται πλέον να εμπιστεύονται κεντρικούς, ανθρώπινους θεσμούς (όπως κεντρικές τράπεζες ή εκκαθαριστικούς οίκους), αλλά αντίθετα βασίζονται στην αδιαμφισβήτητη βεβαιότητα των μαθηματικών αποδείξεων και του ανοιχτού κώδικα (Verifiable Computing). Σε αυτό το πλαίσιο, η εφαρμοσμένη κρυπτογραφία καλείται να εξυπηρετήσει τρεις κεντρικούς άξονες, οι οποίοι επαναπροσδιορίζουν πλήρως τα παραδοσιακά μοντέλα κυβερνοασφάλειας:

- **Ακεραιότητα Δεδομένων (Data Integrity) και Συναρτήσεις Κατακερματισμού:** Σε μια παραδοσιακή, κεντροποιημένη σχεσιακή βάση δεδομένων, η ακεραιότητα των εγγραφών εξαρτάται απόλυτα από τα δικαιώματα πρόσβασης του διαχειριστή συστήματος (system administrator). Στα κατανεμημένα καθολικά, η ακεραιότητα διασφαλίζεται αλγοριθμικά μέσω Μονόδρομων Συναρτήσεων Κατακερματισμού (Cryptographic Hash Functions), όπως ο αλγόριθμος SHA-256 στο Bitcoin ή ο Keccak-256 στο Ethereum. Κάθε παραγόμενο μπλοκ περιέχει ενσωματωμένο το κρυπτογραφικό αποτύπωμα (hash) της κεφαλίδας του ακριβώς προηγούμενου μπλοκ, δημιουργώντας μια αδιάσπαστη χρονολογική αλυσίδα. Οι αλγόριθμοι αυτοί διέπονται από το «Φαινόμενο της Χιονοστιβάδας» (Avalanche Effect): οποιαδήποτε ελάχιστη απόπειρα αναδρομικής αλλοίωσης μιας συναλλαγής (έστω και η αλλαγή ενός ψηφίου σε ένα ποσό μεταφοράς) αλλάζει ριζικά το τελικό αποτύπωμα του μπλοκ. Αυτό καταστρέφει άμεσα τη συνοχή όλων των επόμενων μπλοκ, καθιστώντας την προσπάθεια απάτης (tampering) ακαριαία ορατή και αυτομάτως απορριπτέα από τον μηχανισμό συναίνεσης των κόμβων του δικτύου. Παράλληλα, η χρήση δομών όπως τα Δέντρα Merkle (Merkle Trees) επιτρέπει την ταχύτατη και αποδοτική επαλήθευση της ακεραιότητας τεράστιου όγκου δεδομένων, χωρίς να απαιτείται η σάρωση ολόκληρης της βάσης.
- **Μη-Αρνησιμότητα (Non-Repudiation) μέσω Ασύμμετρης Κρυπτογραφίας:** Η μη-αρνησιμότητα αποτελεί την ιδιότητα εκείνη που αποτρέπει έναν χρήστη από το να αμφισβητήσει εκ των υστέρων τη γνησιότητα μιας ενέργειας που ο ίδιος πραγματοποίησε. Στο οικοσύστημα των κρυπτονομισμάτων, η ιδιότητα αυτή υλοποιείται αποκλειστικά μέσω της Κρυπτογραφίας Δημοσίου Κλειδιού (Public Key Cryptography - PKC) και των Ψηφιακών Υπογραφών (Digital Signatures). Ειδικότερα, χρησιμοποιείται ο Αλγόριθμος Ψηφιακής Υπογραφής Ελλειπτικών Καμπυλών (ECDSA), ο οποίος παρέχει ύψιστη ασφάλεια με μικρότερο μέγεθος κλειδιού σε σύγκριση με παραδοσιακά συστήματα όπως το RSA. Όταν ένας χρήστης εκπέμπει (broadcasts) μια συναλλαγή μεταφοράς αξίας στο δίκτυο, την υπογράφει κρυπτογραφικά χρησιμοποιώντας το μυστικό, ιδιωτικό του Κλειδί (Private Key). Αυτή η διαδικασία λειτουργεί ως μια μαθηματική "συνάρτηση καταπακτής" (trapdoor function): είναι υπολογιστικά αδύνατον για έναν κακόβουλο χρήστη να πλαστογραφήσει την υπογραφή χωρίς το ιδιωτικό κλειδί, αλλά είναι υπολογιστικά ασήμαντο για οποιονδήποτε κόμβο του δικτύου να επαληθεύσει την εγκυρότητά της χρησιμοποιώντας απλώς το Δημόσιο Κλειδί του αποστολέα. Η ύπαρξη μιας έγκυρης ψηφιακής υπογραφής αποτελεί αδιάσειστη νομική και τεχνική απόδειξη πρόθεσης.

- **Αυθεντικοποίηση Χωρίς Ταυτότητα (Authentication without Identity) και Αυτο-Φύλαξη:** Ίσως η πλέον ριζοσπαστική καινοτομία του Blockchain είναι ο πλήρης εννοιολογικός διαχωρισμός της ταυτότητας (Identity) από την ιδιοκτησία (Ownership). Στο παραδοσιακό νομισματικό σύστημα, η αυθεντικοποίηση προϋποθέτει την αποκάλυψη της ταυτότητας μέσω αυστηρών διαδικασιών ταυτοποίησης (KYC - Know Your Customer). Αντιθέτως, η αρχιτεκτονική του Blockchain εισάγει το μοντέλο της "Ψευδωνυμίας" (Pseudonymity). Το δίκτυο αγνοεί παντελώς το φυσικό πρόσωπο που εκτελεί τη συναλλαγή· δεν ενδιαφέρεται για το "ποιος είναι" ο χρήστης, αλλά αποκλειστικά για το "τι κατέχει". Η διεύθυνση ενός πορτοφολιού είναι απλώς μια παραγόμενη μορφή (hash) του δημόσιου κλειδιού, και η κατοχή του αντίστοιχου Ιδιωτικού Κλειδιού (Self-Custody) είναι η απόλυτη και μοναδική προϋπόθεση για τη διαχείριση των κεφαλαίων. Αυτή η αρχή κωδικοποιείται από τη βιομηχανία με το ρητό «Not your keys, not your coins», αναδεικνύοντας ότι σε ένα αποκεντρωμένο περιβάλλον, η κρυπτογραφική εξουσιοδότηση υποκαθιστά πλήρως την ανάγκη για ανθρώπινη επιβεβαίωση ταυτότητας.

5.2 Ασύμμετρη Κρυπτογραφία και Ελλειπτικές Καμπύλες (ECC)

Ενώ η αρχιτεκτονική του πρώιμου διαδικτύου και των συμβατικών τραπεζικών συστημάτων βασίστηκε για δεκαετίες στον αλγόριθμο RSA (Rivest–Shamir–Adleman) και στο μαθηματικό πρόβλημα της παραγοντοποίησης τεράστιων πρώτων αριθμών, η βιομηχανία των αποκεντρωμένων δικτύων και των κρυπτονομισμάτων υιοθέτησε σχεδόν καθολικά —από την πρώτη ημέρα της γένεσής της— την Κρυπτογραφία Ελλειπτικών Καμπυλών (Elliptic Curve Cryptography - ECC). Η επιλογή αυτή δεν αποτέλεσε μια τυχαία τεχνολογική μετάβαση, αλλά υπαγορεύτηκε από τις αυστηρές απαιτήσεις απόδοσης των κατανεμημένων καθολικών.

Η τεχνολογία ECC προσφέρει το ίδιο ή και υψηλότερο επίπεδο κρυπτογραφικής ασφάλειας με το RSA, αλλά με δραματικά μικρότερο μέγεθος κλειδιού. Για παράδειγμα, ένα κλειδί ECC μήκους 256 bits παρέχει ισοδύναμη προστασία με ένα κλειδί RSA μήκους 3072 bits. Αυτή η δραστηρική συμπίεση των δεδομένων είναι απολύτως κρίσιμη σε ένα περιβάλλον Blockchain, όπου κάθε ψηφιακή υπογραφή πρέπει να αποθηκεύεται μόνιμα από χιλιάδες κόμβους. Η μείωση του μεγέθους μεταφράζεται άμεσα σε εξοικονόμηση αποθηκευτικού χώρου, ταχύτερους χρόνους επαλήθευσης των συναλλαγών (transaction verification times) και ελαχιστοποίηση των απαιτήσεων εύρους ζώνης (bandwidth) για τη διάδοση των μπλοκ στο παγκόσμιο δίκτυο (P2P network). Ειδικότερα, κορυφαία πρωτόκολλα όπως το Bitcoin και το Ethereum, κάνουν χρήση της τυποποιημένης καμπύλης secp256k1 (βάσει των προτύπων του οργανισμού SEC2), η οποία βελτιστοποιήθηκε για μέγιστη αποδοτικότητα στον υπολογισμό κρυπτογραφικών υπογραφών (ECDSA).

5.2.1 Το Πρόβλημα του Διακριτού Λογαρίθμου (ECDLP) και η Μαθηματική Θεμελίωση

Η δομική ασφάλεια της Κρυπτογραφίας Ελλειπτικών Καμπυλών δεν βασίζεται στη μυστικότητα του αλγορίθμου (σύμφωνα με την αρχή του Kerckhoffs), αλλά στην τεράστια υπολογιστική δυσκολία επίλυσης του Προβλήματος του Διακριτού Λογαρίθμου σε Ελλειπτικές Καμπύλες (Elliptic Curve Discrete Logarithm Problem - ECDLP). Σε αυστηρό μαθηματικό επίπεδο, μια ελλειπτική καμπύλη ορίζεται πάνω σε ένα πεπερασμένο σώμα πρώτου αριθμού $\mathbb{F}_p$ από την εξίσωση Weierstrass:

$$y^2 = x^3 + ax + b \pmod{p}$$

Η βασική εξίσωση παραγωγής κλειδιών, η οποία αποτελεί τον πυρήνα της δημιουργίας κάθε ψηφιακού πορτοφολιού και διέπει την ιδιοκτησία των περιουσιακών στοιχείων, ορίζεται ως:

$$Q = k \times G$$

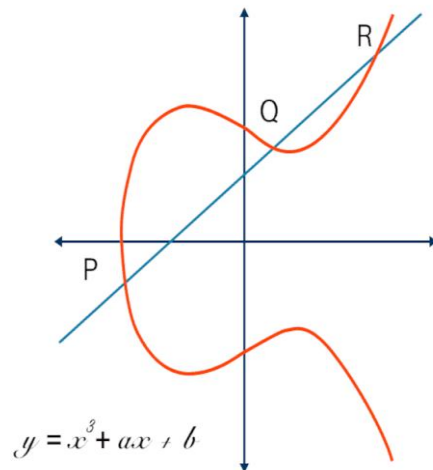
Σε αυτή την αλγεβρική σχέση, οι μεταβλητές ορίζονται ως εξής:

- k (**Ιδιωτικό Κλειδί**): Ένας τυχαία παραγόμενος, κολοσσιαίος ακέραιος αριθμός των 256 bits, τον οποίο ο χρήστης οφείλει να διατηρεί απολύτως μυστικό.
- G (**Σημείο Γεννήτορας - Generator Point**): Μια σταθερή, παγκοσμίως γνωστή συντεταγμένη πάνω στην ελλειπτική καμπύλη, προκαθορισμένη από το πρωτόκολλο.
- Q (**Δημόσιο Κλειδί**): Το παραγόμενο σημείο που προκύπτει πάνω στην ίδια ελλειπτική καμπύλη, το οποίο μοιράζεται ελεύθερα στο δίκτυο.

Πρέπει να τονιστεί ότι η μαθηματική πράξη $k \times G$ δεν αποτελεί έναν απλό βαθμωτό πολλαπλασιασμό, όπως συμβαίνει στη συμβατική αριθμητική. Αντιθέτως, εκφράζει τον Πολλαπλασιασμό Βαθμωτού (Scalar Multiplication) σε γεωμετρικό χώρο, ο οποίος υλοποιείται αλγοριθμικά ως μια αλληλουχία διαδοχικών προσθέσεων του σημείου G στον εαυτό του, k φορές ($G + G + G \dots + G$).

Η "μαγεία" και η κρυπτογραφική ισχύς αυτής της εξίσωσης έγκειται στην εγγενώς μονόδρομη φύση της, λειτουργώντας ως "Συνάρτηση Καταπακτής" (Trapdoor Function). Ενώ ο υπολογισμός της κατευθυνόμενης πορείας —δηλαδή ο πολλαπλασιασμός του k με το G για την παραγωγή του Δημόσιου Κλειδιού Q — είναι μια υπολογιστικά τετριμμένη και εξαιρετικά γρήγορη πράξη για τους σύγχρονους επεξεργαστές (συχνά αξιοποιώντας αλγορίθμους "Double-and-Add"), η αντίστροφη διαδικασία είναι απαγορευτική.

Η προσπάθεια εύρεσης του μυστικού ακεραίου k , γνωρίζοντας αποκλειστικά τις συντεταγμένες του παραγόμενου σημείου Q και του αρχικού σημείου G , συνεπάγεται τη μαθηματική διαίρεση στην καμπύλη, μια πράξη που δεν υφίσταται. Μέχρι σήμερα, δεν υπάρχει κανένας γνωστός αλγόριθμος υπο-εκθετικού χρόνου (sub-exponential time algorithm) ικανός να επιλύσει το πρόβλημα ECDLP. Η παραβίαση ενός κλειδιού 256 bits μέσω επίθεσης ωμής βίας (brute force) ή μέσω προηγμένων αλγορίθμων (όπως ο αλγόριθμος Pollard's rho) απαιτεί την εκτέλεση ενός αδιανόητου αριθμού συνδυασμών. Οι ενεργειακοί πόροι και ο χρόνος που θα απαιτούνταν για την αντιστροφή αυτής της εξίσωσης, ακόμη και από ένα παγκόσμιο δίκτυο υπερυπολογιστών, υπερβαίνουν την ενέργεια που διαθέτει ολόκληρο το ηλιακό μας σύστημα, καθιστώντας τα κεφάλαια των χρηστών θεωρητικά και πρακτικά απαραβίαστα.



Εικόνα 11: Γραφική αναπαράσταση μιας Ελλειπτικής Καμπύλης (ECC) πάνω στην οποία βασίζεται η ασύμμετρη παραγωγή δημοσίων κλειδίων.

5.2.2 Συγκριτική Ανάλυση

Αποδοτικότητα: RSA έναντι ECC

Η απόλυτη επικράτηση της Κρυπτογραφίας Ελλειπτικών Καμπυλών (ECC) έναντι του παραδοσιακού αλγορίθμου RSA δεν ήταν τυχαία, αλλά αποτέλεσμα της επιτακτικής ανάγκης για βελτιστοποίηση των υπολογιστικών πόρων στα κατανεμημένα δίκτυα. Η βασική διαφορά εντοπίζεται στο μέγεθος του κλειδιού που απαιτείται για την επίτευξη του ίδιου επιπέδου ασφαλείας.

Καθώς το πρόβλημα της παραγοντοποίησης πρώτων αριθμών (στο οποίο βασίζεται ο RSA) είναι υπολογιστικά πιο εύκολο από το πρόβλημα ECDLP της ECC, ο αλγόριθμος RSA απαιτεί εκθετικά μεγαλύτερα κλειδιά για να παραμείνει αδιαπέραστος. Για παράδειγμα, προκειμένου να επιτευχθεί ένα αποδεκτό επίπεδο ασφαλείας 128 bits, ο RSA απαιτεί ένα εξαιρετικά δυσκίνητο κλειδί μεγέθους 3072 bits. Αντιθέτως, η ECC προσφέρει την ίδια ακριβώς αδιαπέραστη προστασία με ένα κλειδί μεγέθους μόλις 256 bits (μια αναλογία 1 προς 12). Αυτή η τεράστια διαφορά μεγέθους είναι καθοριστική για την απόδοση του Blockchain, διότι μικρότερα

κλειδιά μεταφράζονται σε μικρότερα μεγέθη συναλλαγών, μικρότερη κατανάλωση μνήμης στους σκληρούς δίσκους των κόμβων (ledger size) και απείρως ταχύτερη επαλήθευση των υπογραφών από συσκευές περιορισμένης ισχύος, όπως τα κινητά τηλέφωνα.

Αξίζει να σημειωθεί ότι το Bitcoin, μέσα από τον κώδικα του Satoshi Nakamoto, χρησιμοποιεί μια πολύ συγκεκριμένη ελλειπτική καμπύλη, γνωστή ως secp256k1 (Koblitz curve). Η επιλογή αυτή, αντί για τις τυπικές καμπύλες που πρότεινε το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ (NIST), φημολογείται πως έγινε ενσυνείδητα ώστε να αποφευχθεί κάθε πιθανότητα ύπαρξης ενσωματωμένης "κερκόπορτας" (backdoor) από κυβερνητικές υπηρεσίες ασφαλείας, καθώς οι παράμετροι της Koblitz curve είναι μαθηματικά αυστηρά προβλέψιμες και όχι παραγόμενες από άγνωστους "τυχαίους" σπόρους.

5.3 Μηχανισμοί Ψηφιακών Υπογραφών (Digital Signature Schemes)

Στο περιβάλλον των αποκεντρωμένων δικτύων και των κρυπτονομισμάτων, η ψηφιακή υπογραφή αποτελεί το μοναδικό και αποκλειστικό κρυπτογραφικό εργαλείο που εξουσιοδοτεί οποιαδήποτε μετάβαση κατάστασης (state transition) και μεταφορά αξίας. Ένα τυπικό σχήμα ψηφιακής υπογραφής αποτελείται από τρεις αλγόριθμους: την παραγωγή ζεύγους κλειδίων (KeyGen), την παραγωγή της υπογραφής (Sign) και την επαλήθευση (Verify). Ωστόσο, οι υποκείμενοι αλγόριθμοι που υλοποιούν αυτές τις συναρτήσεις έχουν εξελιχθεί ραγδαία, προκειμένου να ανταποκριθούν στις αυστηρές απαιτήσεις κλιμάκωσης και ιδιωτικότητας του Web3.

5.3.1 Ο Αλγόριθμος ECDSA και η Κρίσιμη Ευπάθεια του Τυχαίου Nonce

Ο Αλγόριθμος Ψηφιακής Υπογραφής Ελλειπτικών Καμπυλών (ECDSA - Elliptic Curve Digital Signature Algorithm) αποτελεί το ιστορικό πρότυπο (standard) που υιοθετήθηκε αρχικά από τον δημιουργό του Bitcoin (Satoshi Nakamoto) και μεταγενέστερα ενσωματώθηκε απaráλλακτο στο Ethereum. Μια έγκυρη υπογραφή ECDSA αποτελείται από ένα ζεύγος τιμών (r, s) .

Κατά τη διαδικασία παραγωγής της τιμής s , ο αλγόριθμος απαιτεί την αυστηρή επιλογή ενός κρυπτογραφικά ασφαλούς, απολύτως τυχαίου και εφήμερου ακέραιου αριθμού k (γνωστού ως cryptographic nonce). Η μαθηματική εξίσωση της υπογραφής ορίζεται ως εξής:

$$s = k^{-1}(z + r \cdot d) \pmod{n}$$

όπου z είναι το κατακερματισμένο αποτύπωμα (hash) της συναλλαγής, d είναι το απόλυτα μυστικό Ιδιωτικό Κλειδί του χρήστη, και n είναι η τάξη της ελλειπτικής καμπύλης.

Εδώ ακριβώς εντοπίζεται η «Αχιλλέως πτέρνα» του ECDSA, η οποία έχει οδηγήσει στην απώλεια κεφαλαίων εκατομμυρίων δολαρίων ιστορικά. Εάν η Γεννήτρια Τυχαίων Αριθμών (RNG) του ψηφιακού πορτοφολιού παρουσιάσει έλλειψη εντροπίας (low entropy) και χρησιμοποιήσει την ίδια ακριβώς τιμή k για την υπογραφή δύο διαφορετικών συναλλαγών (έστω z_1 και z_2), προκύπτει μια καταστροφική κρυπτογραφική σύγκρουση. Οι παραγόμενες υπογραφές θα έχουν την ίδια τιμή r , αλλά διαφορετικά s_1 και s_2 .

Ένας επιτιθέμενος (ή ένα αυτοματοποιημένο bot παρακολούθησης του blockchain), παρατηρώντας απλώς τις δημόσιες συναλλαγές, μπορεί να αφαιρέσει τις δύο εξισώσεις και να υπολογίσει άμεσα το μυστικό nonce k :

$$k = \frac{z_1 - z_2}{s_1 - s_2} \pmod{n}$$

Γνωρίζοντας πλέον το k , η εύρεση του μυστικού Ιδιωτικού Κλειδιού (d) του χρήστη επιλύεται μέσω στοιχειώδους άλγεβρας:

$$d = \frac{s_1 \cdot k - z_1}{r} \pmod{n}$$

Αυτή η μαθηματική ευπάθεια σημαίνει ότι ένα μικρό σφάλμα στο λογισμικό παραγωγής τυχαιότητας οδηγεί σε ολοκληρωτική και ακαριαία κλοπή των κεφαλαίων, ανεξάρτητα από το μέγεθος του κωδικού πρόσβασης του χρήστη. Για τον λόγο αυτό, τα σύγχρονα συστήματα απαιτούν την υλοποίηση ντετερμινιστικών αλγορίθμων παραγωγής nonce, σύμφωνα με το πρότυπο RFC 6979.

5.3.2 Υπογραφές Schnorr, Ιδιότητα Γραμμικότητας και η Αναβάθμιση Taproot

Για την οριστική επίλυση των εγγενών περιορισμών και των κινδύνων του ECDSA, το δίκτυο του Bitcoin ενσωμάτωσε πρόσφατα, μέσω της ιστορικής αναβάθμισης Taproot (BIP-340), τον αλγόριθμο υπογραφών Schnorr. Ο αλγόριθμος αυτός, που παρέμενε για χρόνια υπό το καθεστώς πατέντας, θεωρείται πλέον το απόλυτο state-of-the-art της εφαρμοσμένης κρυπτογραφίας, προσφέροντας ανώτερες μαθηματικές αποδείξεις ασφαλείας.

Το κορυφαίο, ριζοσπαστικό πλεονέκτημα του αλγορίθμου Schnorr είναι η θεμελιώδης μαθηματική ιδιότητα της Γραμμικότητας (Linearity). Σε αντίθεση με τον ECDSA, ο οποίος παράγει κατακερματισμένες και μη προσθετικές υπογραφές, οι αλγόριθμοι Schnorr επιτρέπουν την απευθείας αλγεβρική άθροιση των κλειδιών. Πρακτικά, η ιδιότητα αυτή μεταφράζεται στη σχέση:

$$\text{Sign}(k_1) + \text{Sign}(k_2) = \text{Sign}(k_1 + k_2)$$

Η γραμμικότητα αυτή επιτρέπει τη λειτουργία της Συσσωμάτωσης Κλειδιών (Key Aggregation) μέσω πρωτοκόλλων όπως το MuSig. Εάν τρεις διαφορετικοί χρήστες (ή τρία διαφορετικά ιδρύματα) επιθυμούν να δημιουργήσουν έναν κοινό λογαριασμό Πολλαπλών Υπογραφών (Multi-Signature Wallet, π.χ. ένα σχήμα 3-από-3), στο παλιό σύστημα P2SH (Pay-to-Script-Hash) έπρεπε να αναρτηθούν στο δημόσιο Blockchain και τα τρία δημόσια κλειδιά καθώς και οι τρεις ξεχωριστές υπογραφές (ECDSA). Αυτή η αρχιτεκτονική σπαταλούσε τεράστιο, πολύτιμο χώρο στο μπλοκ (αυξάνοντας δραματικά τα τέλη δικτύου - gas fees) και αποκάλυπτε την πλήρη δομή της συνδιαλλαγής σε τρίτους.

Με την υιοθέτηση των υπογραφών Schnorr, οι χρήστες συνδυάζουν διαδραστικά τα επιμέρους δημόσια κλειδιά τους εκτός αλυσίδας (off-chain), παράγοντας ένα ενιαίο, συλλογικό Δημόσιο Κλειδί. Αντίστοιχα, παράγουν μία και μοναδική «συσσωματωμένη» υπογραφή. Όταν αυτή η υπογραφή αναρτηθεί στο δίκτυο για επικύρωση, είναι κρυπτογραφικά δυσδιάκριτη από μια τυπική συναλλαγή ενός απλού, μεμονωμένου χρήστη.

Αυτή η εξέλιξη επιφέρει δύο καταλυτικά αποτελέσματα: αφενός ελαττώνει τον όγκο των δεδομένων κατά τουλάχιστον 20% (επιτυγχάνοντας On-chain Scalability), και αφετέρου προσφέρει απόλυτη ιδιωτικότητα. Εξαλείφει πλήρως την ικανότητα εταιρειών ανάλυσης της αλυσίδας (όπως η Chainalysis) να διακρίνουν εάν μια κίνηση κεφαλαίων προήλθε από έναν μεμονωμένο επενδυτή, από ένα πολύπλοκο εταιρικό έξυπνο συμβόλαιο ή από το δίκτυο Lightning (Layer 2), ενισχύοντας θεαματικά την ομοιογένεια και την ανταλλαξιμότητα (fungibility) των νομισμάτων.

5.4 Διαχείριση Κλειδιών, Ιεραρχικά Ντετερμινιστικά Πορτοφόλια και Πρότυπα BIP

Όσο ισχυρό και αν είναι το υποκείμενο μαθηματικό μοντέλο ενός κρυπτοσυστήματος, η συνολική του ασφάλεια υποβαθμίζεται εάν ο τελικός χρήστης αδυνατεί να διαχειριστεί, να αποθηκεύσει και να ανακτήσει τα κρυπτογραφικά του κλειδιά με ασφάλεια. Στα πρώτα στάδια ανάπτυξης του Bitcoin, τα ψηφιακά πορτοφόλια (γνωστά ως πορτοφόλια Τύπου-0 ή Non-Deterministic Wallets) παρήγαγαν εντελώς τυχαία, ανεξάρτητα ζεύγη κλειδιών για κάθε νέα συναλλαγή, εφαρμόζοντας την πρακτική JBOK (Just a Bunch Of Keys) [11]. Η αρχιτεκτονική αυτή εγκυμονούσε τεράστιους κινδύνους: ο χρήστης όφειλε να δημιουργεί αδιάκοπα νέα αντίγραφα ασφαλείας (backups) του σκληρού του δίσκου. Εάν ο υπολογιστής του κατέρρεε πριν προλάβει να αποθηκεύσει το πιο πρόσφατο παραγόμενο κλειδί, τα κεφάλαια που συνδέονταν με αυτό χάνονταν οριστικά.

Η οριστική επίλυση αυτού του τεχνικού αδιεξόδου επήλθε μέσω της τυποποίησης πρωτοκόλλων, γνωστών ως Προτάσεις Βελτίωσης του Bitcoin (Bitcoin Improvement Proposals - BIPs), τα οποία πλέον αποτελούν το θεμελιώδες βιομηχανικό πρότυπο για το σύνολο των κρυπτονομισμάτων [11].

5.4.1 BIP-32: Ιεραρχικά Ντετερμινιστικά Πορτοφόλια (HD Wallets)

Το πρότυπο BIP-32 εισήγαγε τα Ιεραρχικά Ντετερμινιστικά Πορτοφόλια (Hierarchical

Deterministic Wallets). Αντί για τη σποραδική και άναρχη παραγωγή κλειδιών, η τεχνολογία αυτή χρησιμοποιεί μια δένδρική δομή (tree structure). Όλα τα κλειδιά ενός χρήστη (ακόμα και αν ανέρχονται σε εκατομμύρια διευθύνσεις) παράγονται αλγοριθμικά και ντετερμινιστικά από έναν και μοναδικό «Κύριο Σπόρο» (Master Seed) των 512 bits [11]. Μέσω της συνάρτησης μονόδρομου κατακερματισμού HMAC-SHA512, ο αρχικός σπόρος παράγει ένα Κύριο Ιδιωτικό Κλειδί (Master Private Key) και έναν Κωδικό Κύριας Αλυσίδας (Master Chain Code).

Από αυτόν τον κεντρικό κόμβο, μπορούν να προκύψουν πρακτικά άπειρα «κλειδιά-παιδιά» (child keys). Ένα κρίσιμο πλεονέκτημα αυτής της αρχιτεκτονικής είναι η ικανότητα παραγωγής Εκτεταμένων Δημόσιων Κλειδιών (Extended Public Keys - xpub). Μέσω αυτών, ένας διακομιστής ηλεκτρονικού εμπορίου (e-commerce server) μπορεί να παράγει ατελείωτες νέες διευθύνσεις λήψης πληρωμών για τους πελάτες του, χωρίς να έχει καμία απολύτως πρόσβαση στα αντίστοιχα ιδιωτικά κλειδιά, εκμηδενίζοντας τον κίνδυνο κλοπής σε περίπτωση παραβίασης του διακομιστή (web server hack).

5.4.2 BIP-39: Μνημονικές Φράσεις και Κωδικοποίηση Εντροπίας

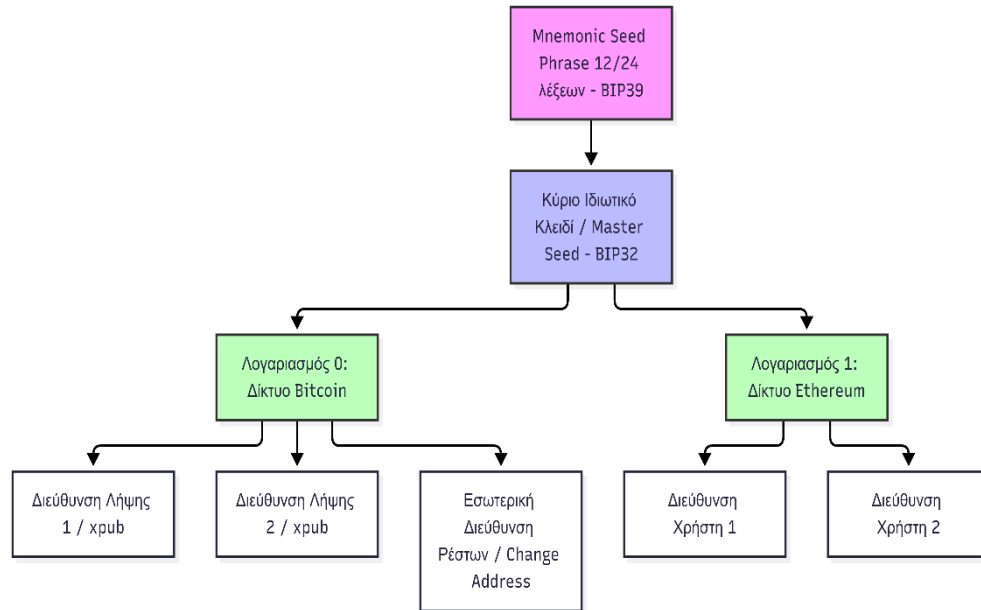
Καθώς ο ανθρώπινος εγκέφαλος είναι εξελικτικά ανίκανος να απομνημονεύσει και να μεταγράψει χωρίς σφάλματα μια ακαταλαβίστικη σειρά 64 δεκαεξαδικών χαρακτήρων, το πρότυπο BIP-39 γεφύρωσε το χάσμα μεταξύ μηχανής και χρήστη. Το πρότυπο αυτό τυποποίησε τη διαδικασία μετατροπής της ακατέργαστης τυχαιότητας (Εντροπία 128 έως 256 bits) σε μια ακολουθία φυσικών, αναγνώσιμων λέξεων, δημιουργώντας τη Μνημονική Φράση (Mnemonic Phrase / Seed Phrase).

Η διαδικασία είναι αυστηρά μαθηματική: το αρχικό τυχαίο μέγεθος συνδυάζεται με ένα άθροισμα ελέγχου (checksum), τεμαχίζεται σε τμήματα των 11 bits και κάθε τμήμα αντιστοιχίζεται σε μια λέξη από ένα προκαθορισμένο, παγκόσμιο λεξικό 2048 αγγλικών λέξεων [11]. Το αποτέλεσμα είναι μια φράση 12 έως 24 λέξεων. Στη συνέχεια, η φράση αυτή περνάει μέσα από τη συνάρτηση παραγωγής κλειδιών PBKDF2 (Password-Based Key Derivation Function 2), εκτελώντας 2048 επαναλήψεις της HMAC-SHA512 προκειμένου να παραχθεί ο τελικός «Κύριος Σπόρος» των 512 bits. Συνεπώς, η φυσική κατοχή αυτών των λέξεων γραμμένων σε ένα ασφαλές μέσο (π.χ. σε χαρτί ή χαραγμένων σε μέταλλο), ισοδυναμεί απόλυτα και μαθηματικά με την ιδιοκτησία των περιουσιακών στοιχείων στο δίκτυο, επιτρέποντας την ανάκτησή τους σε οποιαδήποτε συσκευή, οπουδήποτε στον κόσμο, ακόμα και αν το αρχικό υλικό (hardware) καταστραφεί.

5.4.3 BIP-44: Πολυ-Νομισματική Οργάνωση (Multi-Account Hierarchy)

Για την οργάνωση του χαώδους δέντρου διευθύνσεων που δημιουργεί το BIP-32, το πρότυπο BIP-44 όρισε μια αυστηρή διαδρομή παραγωγής κλειδιών (Derivation Path) της μορφής: `m / purpose' / coin_type' / account' / change / address_index` [11].

Αυτή η ιεραρχία επιτρέπει σε ένα μόνο πορτοφόλι, χρησιμοποιώντας την ίδια ακριβώς φράση 24 λέξεων, να διαχειρίζεται ταυτόχρονα και εντελώς ξεχωριστά εκατοντάδες διαφορετικά κρυπτονομίσματα (π.χ. Bitcoin, Ethereum, Solana) και πολλαπλούς λογαριασμούς ελέγχου και ταμειυτηρίου για το καθένα. Εάν ο χρήστης χρειαστεί να ανακτήσει το πορτοφόλι του, το λογισμικό θα σαρώσει αυτόματα αυτή την τυποποιημένη διαδρομή, εντοπίζοντας άμεσα πού βρίσκονται τα κεφάλαια σε κάθε διαφορετικό Blockchain.



Εικόνα 12: Δενδρική αρχιτεκτονική ενός Ιεραρχικά Ντετερμινιστικού (HD) Πορτοφολιού βάσει των προτύπων BIP-32 και BIP-39, όπου εκατομμύρια διευθύνσεις παράγονται από έναν Κύριο Σπόρο.

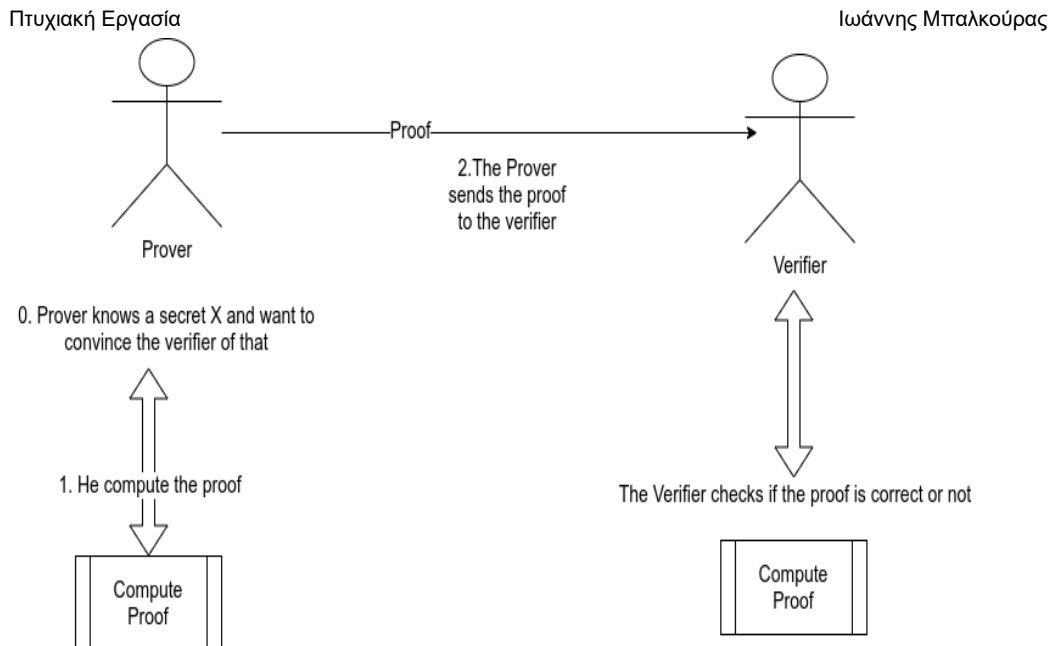
5.5 Προηγμένες Τεχνικές Ιδιωτικότητας και Ανωνυμίας

Μια από τις πλέον διαδεδομένες και επικίνδυνες παρανοήσεις που περιβάλλουν τα δημόσια καταναμεμένα καθολικά (όπως το Bitcoin και το Ethereum) είναι η ψευδαίσθηση της απόλυτης ανωνυμίας. Στην πραγματικότητα, τα δίκτυα αυτά δεν είναι ανώνυμα, αλλά **ψευδώνυμα** και **απολύτως διαφανή**. Κάθε συναλλαγή, το ακριβές ποσό, η χρονική σήμανση (timestamp) και η πλήρης ιστορική διαδρομή των νομισμάτων είναι δημόσια εγγεγραμμένα και διαθέσιμα προς ανάλυση (Chain Analysis) στο διηνεκές. Εάν η ψηφιακή διεύθυνση ενός χρήστη συνδεθεί έστω και μία φορά με την πραγματική του ταυτότητα (π.χ. μέσω ταυτοποίησης KYC σε ένα κεντρικό ανταλλακτήριο), το σύνολο της οικονομικής του συμπεριφοράς αποκαλύπτεται. Προκειμένου να επιτευχθεί πραγματική ιδιωτικότητα επιπέδου μετρητών (cash-like privacy), η επιστήμη της κρυπτογραφίας έχει αναπτύξει τεχνολογίες αιχμής, οι οποίες θολώνουν ή αποκόπτουν πλήρως την αλυσίδα της ιχνηλασιμότητας [39].

5.5.1 Αποδείξεις Μηδενικής Γνώσης (Zero-Knowledge Proofs - ZKP)

Οι Αποδείξεις Μηδενικής Γνώσης (ZKPs) συνιστούν, ίσως, την πλέον επαναστατική εξέλιξη της σύγχρονης θεωρητικής κρυπτογραφίας [36]. Επιτρέπουν σε μια οντότητα, τον Αποδεικνύοντα (Prover), να πείσει μαθηματικά και με απόλυτη βεβαιότητα μια άλλη οντότητα, τον Επαληθευτή (Verifier), ότι μια συγκεκριμένη δήλωση ή υπολογισμός είναι αληθής, χωρίς ωστόσο να του αποκαλύψει **καμία απολύτως άλλη πληροφορία** πέραν της ίδιας της αλήθειας της δήλωσης.

Ένα κλασικό νοητικό πείραμα (thought experiment) για την κατανόηση αυτής της έννοιας είναι η διαδικασία επιβεβαίωσης ηλικίας. Μέσω των ZKPs, ένας πολίτης θα μπορούσε να προσκομίσει σε έναν ελεγκτή μια σύντομη μαθηματική απόδειξη που να πιστοποιεί το γεγονός «Είμαι άνω των 18 ετών», χωρίς να του παραχωρήσει την ταυτότητά του και χωρίς να του αποκαλύψει το όνομά του ή την ακριβή ημερομηνία γέννησής του. Το πρωτόκολλο παράγει μια απάντηση τύπου *True/False* βασισμένη σε κρυπτογραφικές παραμέτρους.



Εικόνα 13: Αρχιτεκτονική διάδρασης μεταξύ Αποδεικνύοντος (Prover) και Επαληθευτή (Verifier) σε ένα πρωτόκολλο Αποδείξεων Μηδενικής Γνώσης (ZKP).

Στην επιστήμη της πληροφορικής, δύο είναι οι κυρίαρχες υλοποιήσεις αυτής της τεχνολογίας, καθεμία με διακριτά αρχιτεκτονικά πλεονεκτήματα:

1. **zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge):** Πρόκειται για την πιο ευρέως χρησιμοποιούμενη κατηγορία. Το κρίσιμο πλεονέκτημά τους είναι η «συνοπτικότητα» (succinctness): η παραγόμενη μαθηματική απόδειξη είναι εξαιρετικά μικρή σε μέγεθος (μερικά bytes) και μπορεί να επαληθευτεί από το Blockchain σε χιλιοστά του δευτερολέπτου. Το μειονέκτημά τους είναι η απαίτηση μιας αρχικής διαδικασίας γνωστής ως «Έμπιστη Εγκατάσταση» (Trusted Setup). Αν τα μέρη που συμμετέχουν στη δημιουργία των αρχικών παραμέτρων του συστήματος δεν καταστρέψουν τα μυστικά τους δεδομένα (toxic waste), θεωρητικά θα μπορούσαν να παραβιάσουν το δίκτυο στο μέλλον, δημιουργώντας χρήματα από το πουθενά [37].
2. **zk-STARKs (Zero-Knowledge Scalable Transparent Argument of Knowledge):** Σχεδιάστηκαν ως απάντηση στην αδυναμία των SNARKs. Τα STARKs είναι απολύτως «διαφανή» (Transparent), καθώς καταργούν την ανάγκη για Trusted Setup, αντλώντας την ασφάλειά τους αποκλειστικά από συμμετρικές συναρτήσεις κατακερματισμού [90]. Αν και οι παραγόμενες αποδείξεις είναι ογκωδέστερες, τα STARKs θεωρούνται εγγενώς ανθεκτικά σε κβαντικές επιθέσεις (Quantum Resistant), καθιστώντας τα θεμελιώδη δομικό λίθο για το μέλλον του συστήματος [82].

5.5.2 Υπηρεσίες Ανάμειξης (Mixers), Έξυπνα Συμβόλαια και το Tornado Cash

Προκειμένου να «σπάσουν» τον κρυπτογραφικό δεσμό (linkability) μεταξύ της διεύθυνσης του αποστολέα και του παραλήπτη, οι χρήστες αξιοποιούν εξειδικευμένες εφαρμογές αποκεντρωμένης ανάμειξης νομισμάτων (Coin Mixers) [40]. Το πιο τεχνολογικά προηγμένο και αμφιλεγόμενο παράδειγμα στο οικοσύστημα του Ethereum υπήρξε το Tornado Cash [47].

Η αρχιτεκτονική του Tornado Cash αποτελεί την επιτομή της εφαρμογής των zk-SNARKs στην ιδιωτικότητα των συναλλαγών. Αντί να προσπαθεί να κρύψει τις συναλλαγές, το έξυπνο συμβόλαιο λειτουργεί ως μια τεράστια, ορατή «μαύρη τρύπα» ρευστότητας. Η λειτουργία του διακρίνεται σε τρία στάδια:

Κατάθεση (Deposit): Ο χρήστης (π.χ. Διεύθυνση Α) καταθέτει ένα σταθερό ποσό (π.χ. 100 ETH) στο έξυπνο συμβόλαιο. Κατά την κατάθεση, ο υπολογιστής του χρήστη παράγει ένα τυχαίο μυστικό (secret) και ένα μηδενικό στοιχείο (nullifier). Στο έξυπνο συμβόλαιο ανεβαίνει μόνο το άθροισμα κατακερματισμού (hash) αυτών των δύο.

1. **Ανάμειξη (Mixing):** Τα κεφάλαια του χρήστη αναμειγνύονται με τα κεφάλαια χιλιάδων άλλων χρηστών σε μια κοινή δεξαμενή, διακόπτοντας την ιχνηλασιμότητα (anonymity set).
2. **Ανάληψη (Withdraw):** Μέρες ή μήνες αργότερα, ο χρήστης δημιουργεί μια ολοκαίνουργια, άδεια Διεύθυνση Β (η οποία δεν έχει καμία ιστορική σύνδεση με τη Διεύθυνση Α). Η Διεύθυνση Β υποβάλλει στο έξυπνο συμβόλαιο μια απόδειξη zk-SNARK και το nullifier. Το δίκτυο (μέσω των αλγορίθμων zk) επιβεβαιώνει μαθηματικά, σε κλάσματα δευτερολέπτου, ότι ο κάτοχος αυτής της απόδειξης έχει κάνει κατάθεση 100 ETH στο παρελθόν και ότι δεν έχει ζητήσει ήδη τα χρήματα (μέσω του nullifier). Το συμβόλαιο απελευθερώνει τα κεφάλαια στη νέα διεύθυνση [47].

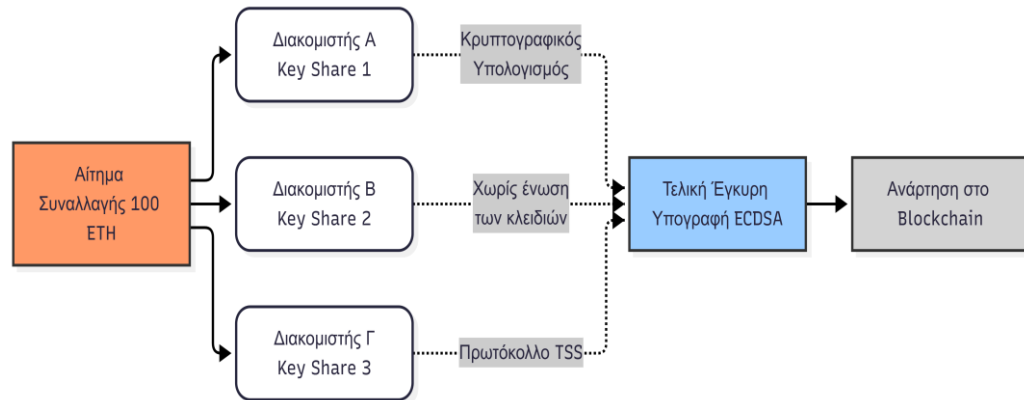
Η ιδιωτικότητα είναι απόλυτη: κανένας αναλυτής και καμία ρυθμιστική αρχή δεν μπορεί να συνδέσει μαθηματικά τη Διεύθυνση Α με τη Διεύθυνση Β. Αυτή ακριβώς η μαθηματική τελειότητα κατέστησε το Tornado Cash εργαλείο επιλογής για ομάδες κυβερνοεγκληματιών (όπως η Lazarus Group της Βόρειας Κορέας) για το ξέπλυμα προϊόντων εγκλήματος, οδηγώντας τελικά στην πρωτοφανή απόφαση του Υπουργείου Οικονομικών των ΗΠΑ (OFAC) να επιβάλει νομικές κυρώσεις, όχι σε ένα φυσικό πρόσωπο ή εταιρεία, αλλά **σε έναν αυτοματοποιημένο, ανοιχτό κώδικα** (open-source smart contract).

5.5.3 Υπολογισμός Πολλαπλών Μερών (Multi-Party Computation - MPC)

Για τους θεσμικούς επενδυτές (Τράπεζες, Αμοιβαία Κεφάλαια, Ανταλλακτήρια) που διαχειρίζονται περιουσιακά στοιχεία δισεκατομμυρίων, η διαχείριση ενός μοναδικού ιδιωτικού κλειδιού αποτελεί τεράστιο συστημικό κίνδυνο (Single Point of Failure - SPoF). Αν το κλειδί διαρρεύσει, κλαπεί ή ο κάτοχός του πέσει θύμα εκβιασμού (η λεγόμενη "\$5 Wrench Attack"), τα κεφάλαια χάνονται ανεπιστρεπτί.

Η κρυπτογραφία Multi-Party Computation (MPC) προσφέρει την απόλυτη τεχνολογική λύση (Enterprise-grade Security). Στη συγκεκριμένη αρχιτεκτονική, το Ιδιωτικό Κλειδί δεν υφίσταται ποτέ στην ολότητά του σε καμία συσκευή. Αντιθέτως, κατά τη φάση της δημιουργίας (Key Generation Phase), το κλειδί γεννιέται εξ αρχής θρυμματισμένο σε ανεξάρτητα, μικρότερα κομμάτια (Key Shares). Τα κομμάτια αυτά διανέμονται και αποθηκεύονται σε γεωγραφικά απομακρυσμένους διακομιστές (servers) και διαφορετικές νομικές οντότητες ανά τον κόσμο.

Προκειμένου να εγκριθεί μια συναλλαγή μεγάλου όγκου, οι επιμέρους διακομιστές επικοινωνούν κρυπτογραφικά, χρησιμοποιώντας πρωτόκολλα όπως το Threshold Signature Scheme (TSS). Υπολογίζουν το μαθηματικό τους μερίδιο και παράγουν μια ενιαία, έγκυρη υπογραφή (συνήθως ECDSA), **χωρίς ποτέ να ενώσουν** τα κομμάτια τους σε έναν κεντρικό υπολογιστή. Αυτό το μοντέλο εξαλείφει την πιθανότητα εσωτερικής απάτης (insider threat) ή μαζικής κλοπής από hackers (data breach), καθώς ένας κυβερνοεγκληματίας θα έπρεπε να παραβιάσει ταυτόχρονα πολλαπλούς, άσχετους μεταξύ τους διακομιστές ανά την υφήλιο, στον ίδιο ακριβώς χρόνο.



Εικόνα 14: Αρχιτεκτονική Υπολογισμού Πολλαπλών Μερών (Multi-Party Computation - MPC) για τη δημιουργία ψηφιακών υπογραφών χωρίς την ανασύσταση του Ιδιωτικού Κλειδιού.

5.6 Η Υπαρξιακή Απειλή των Κβαντικών Υπολογιστών (Y2Q)

Η εμπιστοσύνη της παγκόσμιας οικονομίας (και κατ' επέκταση όλων των κρυπτονομισμάτων) στην ασφάλεια των συστημάτων βασίζεται σε ένα θεμελιώδες μαθηματικό αξίωμα: ότι ορισμένα προβλήματα, όπως η παραγοντοποίηση τεράστιων πρώτων αριθμών (RSA) και ο υπολογισμός του Διακριτού Λογαρίθμου σε Ελλειπτικές Καμπύλες (ECDLP), είναι πρακτικά άλυτα (NP-hard) για τους συμβατικούς (κλασικούς) ηλεκτρονικούς υπολογιστές, ανεξαρτήτως επεξεργαστικής ισχύος [86]. Η ραγδαία εξέλιξη, ωστόσο, της Κβαντικής Πληροφορικής (Quantum Computing) απειλεί να καταρρίψει αυτό το αξίωμα ολοκληρωτικά.

Ενώ οι κλασικοί υπολογιστές επεξεργάζονται πληροφορίες με τη μορφή δυαδικών ψηφίων (Bits) σε κατάσταση 0 ή 1, οι κβαντικοί υπολογιστές αξιοποιούν τα Κβαντικά Bits (Qubits) και φαινόμενα της κβαντομηχανικής, όπως η «Υπέρθωση» (Superposition) και η «Κβαντική Διεμπλοκή» (Entanglement). Αυτό τους επιτρέπει να επεξεργάζονται ταυτόχρονα εκατομμύρια πιθανές καταστάσεις, αυξάνοντας την υπολογιστική τους ισχύ εκθετικά.

Η κρίσιμη απειλή προέρχεται από την ανακάλυψη του **Αλγορίθμου του Shor** (Peter Shor, 1994) [48, 87]. Θεωρητικά, ένας πλήρως λειτουργικός και ανεκτικός σε σφάλματα (fault-tolerant) κβαντικός υπολογιστής με επαρκή αριθμό Qubits, εκτελώντας τον Αλγόριθμο του Shor, δύναται να επιλύσει το πρόβλημα του ECDLP σε **πολυωνυμικό χρόνο** [80]. Αυτό πρακτικά σημαίνει ότι ένας επιτιθέμενος θα μπορούσε να αντλήσει το Δημόσιο Κλειδί οποιουδήποτε χρήστη από το ανοιχτό Blockchain και, μέσα σε λίγα μόλις λεπτά, να υπολογίσει αντίστροφα το αντίστοιχο Ιδιωτικό Κλειδί, αποκτώντας άμεση και αθόρυβη πρόσβαση στα κεφάλαια του θύματος. Ο αντίκτυπος θα ήταν καταστροφικός, οδηγώντας στην κατάρρευση όχι μόνο των ψηφιακών νομισμάτων, αλλά και του παγκόσμιου τραπεζικού και στρατιωτικού συστήματος επικοινωνιών.

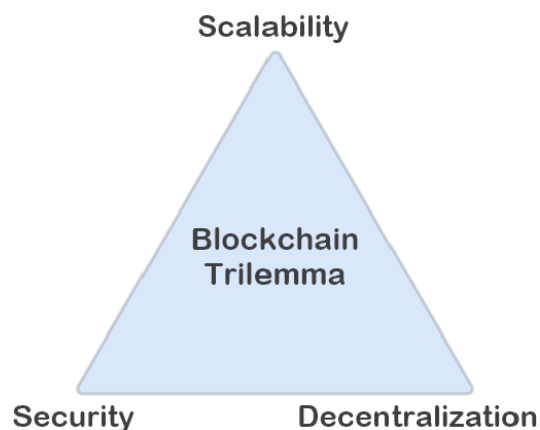
Η βιομηχανία αναφέρεται στην άγνωστη αυτή χρονική στιγμή ως ημερομηνία "Y2Q" (Years to Quantum). Για την αντιμετώπιση αυτής της καταστροφικής, μελλοντικής απειλής, η επιστημονική και κρυπτογραφική κοινότητα (υπό την ηγεσία οργανισμών όπως το NIST) επενδύει ήδη στην ανάπτυξη και τυποποίηση της **Μετα-Κβαντικής Κρυπτογραφίας (Post-Quantum Cryptography - PQC)** [81, 88].

Οι αλγόριθμοι PQC, και ειδικότερα αυτοί που βασίζονται στην **Κρυπτογραφία Πλέγματος (Lattice-based Cryptography)**, εισάγουν μαθηματικά προβλήματα εύρεσης του συντομότερου διανύσματος (Shortest Vector Problem) σε κρυπτογραφικούς χώρους πολλών εκατοντάδων διαστάσεων (multi-dimensional arrays). Τα προβλήματα αυτά θεωρούνται αποδεδειγμένα ανθεκτικά, καθώς δεν μπορούν να επιλυθούν αποδοτικά ούτε καν από τον Αλγόριθμο του Shor [81].

Η τεράστια, υπαρξιακή πρόκληση για τα κορυφαία δίκτυα όπως το Bitcoin και το Ethereum την επόμενη δεκαετία, δεν θα είναι η δημιουργία αυτών των αλγορίθμων, αλλά η "Κρυπτογραφική Ευελιξία" (Crypto-agility): η ικανότητα, δηλαδή, να εφαρμόσουν μια ομαλή και συντονισμένη παγκόσμια αναβάθμιση του λογισμικού τους (Hard Fork), προκειμένου να υιοθετήσουν αυτές τις νέες, ογκωδέστερες κβαντικές υπογραφές, πολύ πριν η απειλή του

6. Προκλήσεις Επεκτασιμότητας, Λύσεις Layer 2 και Διαλειτουργικότητα

Στην επιστήμη των κατανεμημένων συστημάτων είναι ευρέως αποδεκτό ότι δεν υπάρχει καμία απολύτως τεχνολογική επιλογή χωρίς κόστος. Κάθε αρχιτεκτονική απόφαση κατά τον σχεδιασμό ενός δικτύου συνεπάγεται συγκεκριμένους συμβιβασμούς (trade-offs). Το μεγαλύτερο τεχνικό εμπόδιο που αποτρέπει μέχρι σήμερα την καθολική υιοθέτηση της τεχνολογίας Blockchain από το παγκόσμιο χρηματοπιστωτικό σύστημα είναι η αδυναμία ταχείας επεξεργασίας τεράστιου όγκου δεδομένων.



Εικόνα 15: Το Τρίλημμα της Επεκτασιμότητας του Blockchain (Αποκέντρωση, Ασφάλεια, Επεκτασιμότητα).

6.1 Το Τρίλημμα της Επεκτασιμότητας (The Scalability Trilemma)

Ο Vitalik Buterin, συνιδρυτής του Ethereum, τυποποίησε αυτούς τους θεμελιώδεις περιορισμούς, διατυπώνοντας το περίφημο "Τρίλημμα της Επεκτασιμότητας". Το θεώρημα αυτό υποστηρίζει ότι ένα μονολιθικό δίκτυο blockchain καλείται να ισορροπήσει ανάμεσα σε τρεις κρίσιμες ιδιότητες: την Αποκέντρωση (Decentralization), την Ασφάλεια (Security) και την Επεκτασιμότητα (Scalability). Η αυστηρή μαθηματική και δικτυακή πραγματικότητα επιβάλλει ότι το δίκτυο μπορεί να βελτιστοποιήσει ταυτόχρονα μόνο τις δύο από τις τρεις αυτές παραμέτρους. Η προσπάθεια ενίσχυσης της μίας, οδηγεί νομοτελειακά στην υποβάθμιση

τουλάχιστον μίας εκ των άλλων δύο.

Για την πλήρη κατανόηση του προβλήματος, η βιβλιογραφία ορίζει αυστηρά τις τρεις κορυφές αυτού του τριγώνου:

- **Αποκέντρωση (Decentralization):** Αφορά τον βαθμό στον οποίο η επιβίωση του δικτύου δεν εξαρτάται από καμία κεντρική οντότητα ή καρτέλ υπολογιστών. Σε ένα ιδεατό, πλήρως αποκεντρωμένο σύστημα, οποιοσδήποτε χρήστης με βασικό καταναλωτικό εξοπλισμό (consumer hardware) μπορεί να τρέξει έναν πλήρη κόμβο (Full Node) και να επαληθεύσει το ιστορικό όλων των συναλλαγών. Η αποκέντρωση ποσοτικοποιείται συχνά μέσω του "Συντελεστή Nakamoto" (Nakamoto Coefficient), ο οποίος εκφράζει τον ελάχιστο αριθμό ανεξάρτητων οντοτήτων που θα έπρεπε να συνεργαστούν προκειμένου να καταλάβουν το 51% του δικτύου.
- **Ασφάλεια (Security):** Η παράμετρος αυτή αναφέρεται στο τεράστιο οικονομικό ή ενεργειακό κόστος που απαιτείται προκειμένου να παραβιαστεί η ακεραιότητα του καθολικού (Immutability). Σε δίκτυα Proof of Work, η ασφάλεια μετριέται με το συνολικό Hashrate, ενώ σε συστήματα Proof of Stake εξαρτάται από την αξία των δεσμευμένων κεφαλαίων (Staked Value).
- **Επεκτασιμότητα (Scalability):** Αποτελεί την ικανότητα του συστήματος να επεξεργάζεται γεωμετρικά αυξανόμενο όγκο συναλλαγών χωρίς να προκαλείται συμφόρηση, χωρίς να αυξάνεται εκθετικά το κόστος (gas fees) και χωρίς να καθυστερεί η οριστικότητα (latency) της συναλλαγής.

Οι αιτιώδεις σχέσεις που δημιουργούν το Τρίλημμα προκύπτουν από τους φυσικούς περιορισμούς του υλικού. Για να αυξηθεί η ταχύτητα των συναλλαγών (όπως επιχειρούν δίκτυα σαν το Solana ή το Binance Smart Chain), απαιτείται η αύξηση του μεγέθους των παραγόμενων μπλοκ ή η μείωση του χρόνου παραγωγής τους. Ωστόσο, η διαχείριση τεράστιων μπλοκ δεδομένων απαιτεί κολοσσιαία επεξεργαστική ισχύ, αδιανόητο εύρος ζώνης (bandwidth) για τη

διάδοση των δεδομένων και τεράστιο αποθηκευτικό χώρο. Το αποτέλεσμα είναι ότι οι απλοί χρήστες αποκλείονται από τη λειτουργία κόμβων λόγω κόστους, και το δίκτυο καταλήγει να ελέγχεται από ελάχιστα, βιομηχανικά Data Centers. Η αρχιτεκτονική αυτή επιτυγχάνει ταχύτητα, αλλά θυσιάζει ολοκληρωτικά την Αποκέντρωση.

6.2 Λύσεις Πρώτου Επιπέδου (Layer 1 Scaling Solutions)

Προκειμένου να σπάσουν το αδιέξοδο του Τριλήμματος, οι αρχικές προσπάθειες των μηχανικών εστίασαν σε παρεμβάσεις στο Πρώτο Επίπεδο (On-Chain Scaling), τροποποιώντας τους ίδιους τους θεμελιώδεις κανόνες του πρωτοκόλλου μέσω αναβαθμίσεων (Hard Forks).

6.2.1 Αύξηση Μεγέθους Μπλοκ (Block Size Increase) και SegWit

Η πιο προφανής, αλλά εξόχως αμφιλεγόμενη λύση ήταν η αύξηση της χωρητικότητας των μπλοκ. Το 2017, μια ριζοσπαστική μερίδα της κοινότητας του Bitcoin, επιθυμώντας ταχύτερες συναλλαγές, αποσχίστηκε δημιουργώντας το Bitcoin Cash (BCH), αυξάνοντας το όριο δεδομένων από το 1MB στα 8MB. Εντούτοις, η βιβλιογραφία καταδεικνύει ότι η αύξηση του μεγέθους αυξάνει δραματικά τον χρόνο διάδοσης (Propagation Time) μέσα στο παγκόσμιο ίντερνετ. Ένα ογκώδες μπλοκ αργεί να φτάσει από την Ασία στην Ευρώπη, αυξάνοντας κατακόρυφα τον κίνδυνο δημιουργίας "Ορφανών Μπλοκ" (Orphan/Stale Blocks), όταν δύο εξορύκτες βρίσκουν ταυτόχρονα λύση, διασπώντας προσωρινά την αλυσίδα και μειώνοντας την ασφάλεια.

Για τον λόγο αυτό, το κεντρικό δίκτυο του Bitcoin υιοθέτησε μια πιο κομψή προσέγγιση βελτιστοποίησης, το Segregated Witness (SegWit). Ο μηχανισμός αυτός διαχωρίζει τις ογκώδεις κρυπτογραφικές υπογραφές (οι οποίες καταλαμβάνουν το ~65% του χώρου) από τα αμιγή δεδομένα της συναλλαγής, μετακινώντας τις σε μια παράλληλη δομή. Αυτό επέτρεψε την αύξηση της αποτελεσματικής χωρητικότητας (Block Weight) χωρίς την επιβολή επιζήμιων Hard Forks.

6.2.2 Τεμαχισμός Βάσης Δεδομένων (Sharding)

Η πλέον φιλόδοξη αρχιτεκτονική αναδιάρθρωση του Layer 1 είναι το Sharding. Εμπνευσμένη από τις παραδοσιακές βάσεις δεδομένων, η ιδέα καταργεί την απαίτηση κάθε κόμβος να επεξεργάζεται όλες τις συναλλαγές του πλανήτη. Το δίκτυο τεμαχίζεται σε μικρότερες, παράλληλες υπο-αλυσίδες (Shards). Το Shard A επεξεργάζεται το δικό του κομμάτι συναλλαγών εντελώς ανεξάρτητα από το Shard B, προσφέροντας εκθετική Οριζόντια Κλιμάκωση (Horizontal Scaling). Ωστόσο, το Sharding εισάγει το φαινόμενο της "Επίθεσης του 1%": αν το δίκτυο διαιρεθεί σε 100 κομμάτια, ένας χάκερ χρειάζεται πλέον μόνο το 1% της συνολικής ισχύος του δικτύου για να παραβιάσει και να καταλάβει ένα μεμονωμένο Shard, απαιτώντας πολύπλοκους αλγορίθμους τυχαίας ανακατανομής των επικυρωτών (Validators) μέσω μιας κεντρικής αλυσίδας-φάρου (Beacon Chain) για να διατηρηθεί η ασφάλεια.

6.3 Λύσεις Δεύτερου Επιπέδου (Layer 2 Scaling) και Αρθρωτή Αρχιτεκτονική

Λόγω των εγγενών κινδύνων που ενέχει η δομική αλλοίωση του θεμελιώδους πρωτοκόλλου (όπως η αύξηση του μεγέθους των μπλοκ που οδηγεί νομοτελειακά σε υπολογιστική κεντροποίηση), η σύγχρονη ερευνητική κατεύθυνση έχει στραφεί σχεδόν εξ ολοκλήρου στις λύσεις Δεύτερου Επιπέδου (Layer 2). Η κεντρική φιλοσοφία αυτής της προσέγγισης είναι ο αυστηρός διαχωρισμός των αρμοδιοτήτων (Separation of Concerns). Μεταφέρει το τεράστιο υπολογιστικό βάρος της εκτέλεσης των συναλλαγών εκτός της κύριας αλυσίδας (off-chain), αφήνοντας το Layer 1 να λειτουργεί αποκλειστικά ως το τελικό, αδιάφθορο επίπεδο ασφάλειας, επίλυσης διαφορών και εκκαθάρισης (Settlement Layer) [36, 39].

Αυτή η τεχνολογική στροφή γέννησε το παράδειγμα των **Αρθρωτών Δικτύων (Modular Blockchains)**. Αντί ένα ενιαίο δίκτυο να προσπαθεί να εκτελέσει την επεξεργασία (Execution), την ομοφωνία (Consensus) και τη διαθεσιμότητα δεδομένων (Data Availability) ταυτόχρονα — όπως συμβαίνει στα παραδοσιακά "Μονολιθικά" (Monolithic) δίκτυα— η αρχιτεκτονική σπάει σε εξειδικευμένα επίπεδα [41]. Στο πλαίσιο αυτό, έχουν αναπτυχθεί διαφορετικές κατηγορίες λύσεων

Δεύτερου Επιπέδου, η καθεμία με διακριτό μοντέλο ασφαλείας:

6.3.1 Κανάλια Κατάστασης (State Channels)

Τα Κανάλια Κατάστασης αποτέλεσαν την πρώτη ιστορικά προσπάθεια κλιμάκωσης, με το **Lightning Network** του δικτύου Bitcoin να αποτελεί το πιο εμβληματικό παράδειγμα [43]. Η λειτουργία τους βασίζεται στη δημιουργία ενός ιδιωτικού, κρυπτογραφημένου διαύλου επικοινωνίας μεταξύ δύο μερών.

Για το άνοιγμα του καναλιού, τα δύο μέρη καταθέτουν κεφάλαια (collateral) σε ένα Έξυπνο Συμβόλαιο Πολλαπλών Υπογραφών (Multi-signature Wallet) στο Layer 1. Από εκείνη τη στιγμή, μπορούν να ανταλλάξουν εκατομμύρια μικρο-συναλλαγές (micro-transactions) μεταξύ τους εκτός αλυσίδας, ενημερώνοντας απλώς τα ψηφιακά τους υπόλοιπα. Αυτές οι συναλλαγές είναι ακαριαίες και έχουν μηδενικό κόστος, καθώς δεν καταγράφονται στο κύριο δίκτυο. Μόνο όταν τα μέρη αποφασίσουν να κλείσουν το κανάλι, η τελική οικονομική κατάσταση (Final State) υποβάλλεται και καταγράφεται οριστικά στο Layer 1. Αν και εξαιρετικά γρήγορα, τα κανάλια κατάστασης υστερούν στην υποστήριξη πολύπλοκων έξυπνων συμβολαίων (smart contract logic), περιοριζόμενα κυρίως σε απλές, στατικές μεταφορές αξίας.

6.3.2 Πλευρικές Αλυσίδες (Sidechains) έναντι Πραγματικών Layer 2

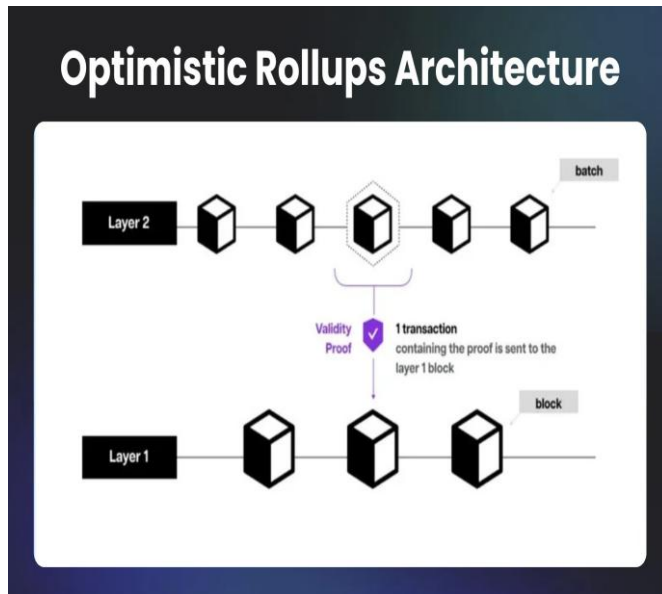
Στη βιβλιογραφία, επικρατεί συχνά σύγχυση μεταξύ των λύσεων Layer 2 και των Πλευρικών Αλυσίδων (Sidechains). Μια πλευρική αλυσίδα είναι ένα απολύτως ανεξάρτητο Blockchain το οποίο τρέχει παράλληλα με το κύριο δίκτυο και συνδέεται με αυτό μέσω μιας αμφίδρομης γέφυρας ρευστότητας (Two-way Bridge).

Η κρίσιμη, ωστόσο, διαφορά εντοπίζεται στο μοντέλο ασφαλείας: μια πλευρική αλυσίδα διαθέτει τους δικούς της κόμβους (validators) και τον δικό της ανεξάρτητο μηχανισμό συναίνεσης. Συνεπώς, εάν το δίκτυο της πλευρικής αλυσίδας δεχθεί κυβερνοεπίθεση ή παραβιαστεί ο αλγόριθμός του (π.χ. μέσω Επίθεσης του 51%), τα κεφάλαια των χρηστών ενδέχεται να κλαπούν ή να παγώσουν. Αντιθέτως, μια πραγματική λύση Layer 2 (όπως τα Rollups) δεν έχει δικό της μηχανισμό συναίνεσης· «κληρονομεί» πλήρως την κρυπτογραφική ασφάλεια του Layer 1. Ακόμα και αν όλοι οι κεντρικοί διακομιστές (sequencers) του Layer 2 καταρρεύσουν, οι χρήστες μπορούν πάντα να ανακτήσουν τα κεφάλαιά τους από το κύριο δίκτυο, μέσω της δημοσιευμένης κατάστασης (State Commitments).

6.3.3 Ο Ρόλος της Διαθεσιμότητας Δεδομένων (Data Availability)

Στις σύγχρονες λύσεις Layer 2 (όπως τα ZK-Rollups και τα Optimistic Rollups που αναλύθηκαν στο κεφάλαιο του αποκεντρωμένου δανεισμού), το μεγαλύτερο εμπόδιο στην απόδοση (bottleneck) δεν είναι πλέον η επεξεργαστική ισχύς (computation), αλλά η Διαθεσιμότητα των Δεδομένων (Data Availability - DA).

Για να είναι ένα Layer 2 απολύτως ασφαλές (trustless), οφείλει να δημοσιεύει τα συμπιεσμένα δεδομένα των συναλλαγών του πίσω στο Layer 1, ώστε οποιοσδήποτε κόμβος του δικτύου να μπορεί να αναδημιουργήσει την πλήρη κατάσταση του συστήματος από το μηδέν και να ελέγξει για τυχόν απάτες. Η αποθήκευση αυτού του τεράστιου όγκου δεδομένων στα παραδοσιακά μπλοκ (calldata) είναι ωστόσο εξαιρετικά δαπανηρή. Η λύση που προκρίνει η έρευνα είναι η δημιουργία εξειδικευμένων δικτύων DA ή τεχνικών διαμοιρασμού δεδομένων (όπως το EIP-4844 Proto-Danksharding στο Ethereum), τα οποία επιτρέπουν την ανάρτηση τεράστιων όγκων "προσωρινών" δεδομένων (blobs) με ελάχιστο κόστος, μετατρέποντας το βασικό Blockchain σε ένα αμιγώς παγκόσμιο επίπεδο επαλήθευσης [41, 42].



Εικόνα 16: Τοπολογική δομή και μετατόπιση του υπολογιστικού φόρτου από το Βασικό Δίκτυο (Layer 1) στις λύσεις Δεύτερου Επιπέδου (Rollups).

6.4 Αρθρωτά Blockchains (Modular Architecture) και Proto-Danksharding

Η παραδοσιακή αρχιτεκτονική του Blockchain χαρακτηρίζεται ως Μονολιθική (Monolithic), καθώς απαιτεί από κάθε υπολογιστή-κόμβο να εκτελεί ταυτόχρονα τέσσερις εξαντλητικές εργασίες: την Εκτέλεση της συναλλαγής, τον Διακανονισμό, την Επίτευξη Συναίνεσης και τη Διαθεσιμότητα Δεδομένων.

Για να ξεπεραστεί αυτό το φράγμα, η σύγχρονη επιστήμη ανέπτυξε την Αρθρωτή (Modular) Αρχιτεκτονική. Σε αυτό το μοντέλο, οι λειτουργίες αποσυνδέονται και ανατίθενται σε εξειδικευμένα δίκτυα. Το Ethereum μετατρέπεται πλέον σε ένα δίκτυο που παρέχει αποκλειστικά Ασφάλεια, Συναίνεση και Διαθεσιμότητα Δεδομένων (Data Availability - DA), αφήνοντας την Εκτέλεση (Execution) και τους πολύπλοκους υπολογισμούς αποκλειστικά στα Rollups.

Το κρίσιμότερο πρόβλημα αυτής της νέας δομής είναι το Πρόβλημα της Διαθεσιμότητας Δεδομένων (DA Problem). Προκειμένου οποιοσδήποτε ελεγκτής να ελέγξει αν ένας Sequencer επιχειρεί απάτη σε ένα Optimistic Rollup, πρέπει να έχει ανεμπόδιστη πρόσβαση στα πρωτογενή δεδομένα. Εάν ο Sequencer αποκρύψει σκόπιμα τα δεδομένα (Data Withholding Attack), το σύστημα είναι αδύνατον να ελεγχθεί. Μέχρι πρότινος, τα Rollups ανέβαζαν όλα αυτά τα δεδομένα στο βασικό δίκτυο του Ethereum (ως call data), κάτι που στοίχιζε αμύθητα ποσά σε τέλη Gas, καθώς οι κόμβοι αναγκάζονταν να τα αποθηκεύουν εσαεί.

Η ιστορική λύση ήρθε με την αναβάθμιση Dencun και το EIP-4844 (Proto-Danksharding). Το πρωτόκολλο αυτό εισήγαγε μια εντελώς νέα δομή δεδομένων, τα Blobs (Binary Large Objects). Τα Blobs είναι "πακέτα" δεδομένων τα οποία προσαρτώνται στα μπλοκ, αλλά αποθηκεύονται στους κόμβους μόνο προσωρινά (για περίπου 18 ημέρες), χρόνο υπεραρκετό για να ελεγχθούν για απάτη, αλλά ιδανικό για να μην επιβαρύνουν μόνιμα τους σκληρούς δίσκους του δικτύου. Η λειτουργία τους θωρακίζεται μέσω προηγμένων Κρυπτογραφικών Δεσμεύσεων Πολυωνύμων KZG (Kate-Zaverucha-Goldberg). Το τελικό στάδιο αυτής της εξέλιξης, το Data Availability Sampling (DAS), θα επιτρέπει στους κόμβους να επιβεβαιώνουν την ύπαρξη τεράστιων όγκων

δεδομένων κατεβάζοντας μόνο ελάχιστα, τυχαία δείγματα (samples), οδηγώντας την ταχύτητα σε εκατομμύρια συναλλαγές ανά δευτερόλεπτο.

6.5 Διαλειτουργικότητα και Γέφυρες Δικτύων (Cross-Chain Bridges)

Καθώς το οικοσύστημα των αποκεντρωμένων τεχνολογιών ωριμάζει, παρατηρείται η ταυτόχρονη ανάδυση πολυάριθμων ισχυρών δικτύων Βασικού (Layer 1) και Δεύτερου Επιπέδου (Layer 2), το καθένα βελτιστοποιημένο για διαφορετικές χρήσεις. Αυτός ο κατακερματισμός οδηγεί στο πρόβλημα των ψηφιακών "σιλό": τεράστιοι όγκοι ρευστότητας και πολύτιμα περιουσιακά στοιχεία (όπως NFTs και Tokens) παραμένουν εγκλωβισμένα σε μεμονωμένα δίκτυα. Από αρχιτεκτονικής άποψης, τα δημόσια Blockchains είναι εκ σχεδιασμού «τυφλά» συστήματα, κλειστού βρόχου. Δεν διαθέτουν εγγενώς την ικανότητα να διαβάσουν, να επιβεβαιώσουν ή να επηρεάσουν την κατάσταση (state) άλλων εξωτερικών δικτύων. Συνεπώς, για τη μεταφορά αξίας και κρυπτογραφικών μηνυμάτων μεταξύ δύο απομονωμένων οικοσυστημάτων, καθίσταται αναγκαία η ανάπτυξη ενδιάμεσων πρωτοκόλλων, γνωστών ως Γεφυρών Διαλειτουργικότητας (Cross-Chain Bridges).

6.5.1 Ο Μηχανισμός Lock-and-Mint και ο Συστημικός Κίνδυνος (Honeypot)

Το πλέον διαδεδομένο τεχνικό πρότυπο για τη μεταφορά νομισμάτων μεταξύ μη συμβατών αλυσίδων είναι το μοντέλο «Κλειδωμα και Έκδοση» (Lock-and-Mint). Εάν ένας χρήστης επιθυμεί, για παράδειγμα, να μεταφέρει Ether (ETH) από το οικοσύστημα του Ethereum στο δίκτυο του Solana, τα νομίσματα στην πραγματικότητα δεν μετακινούνται ποτέ. Αντιθέτως, τα αρχικά ETH κλειδώνονται μόνιμα μέσω μιας συνάρτησης σε ένα έξυπνο συμβόλαιο ("Θησαυροφυλάκιο" / Escrow Vault) στο δίκτυο προέλευσης (Source Chain). Μόλις επιβεβαιωθεί το κλειδωμα, ένα ανεξάρτητο έξυπνο συμβόλαιο στο δίκτυο προορισμού (Destination Chain) λαμβάνει σήμα και εκδίδει (mints) ένα νέο ψηφιακό στοιχείο, το λεγόμενο **"Συσκευασμένο" (Wrapped) Token** (π.χ. WETH). Το token αυτό διατηρεί τεχνητά την ισοτιμία 1:1, καθώς υποστηρίζεται θεωρητικά από τα αντίστοιχα κεφάλαια που βρίσκονται κλειδωμένα στο αρχικό δίκτυο. Η αντίστροφη διαδικασία ονομάζεται Burn-and-Release, όπου τα wrapped tokens καταστρέφονται για να απελευθερωθούν τα αρχικά κεφάλαια.

Ωστόσο, αυτός ο μηχανισμός συγκέντρωσης ρευστότητας δημιουργεί το κλασικό φαινόμενο του "Honeypot" (Δοχείο Μελιού) στον τομέα της κυβερνοασφάλειας. Καθώς οι γέφυρες αυτές συγκεντρώνουν καθημερινά εκατοντάδες εκατομμύρια, ή και δισεκατομμύρια, δολάρια σε κλειδωμένα κεφάλαια εντός ενός και μόνο έξυπνου συμβολαίου, αποτελούν τον νούμερο ένα στόχο εξελιγμένων κυβερνοεπιθέσεων (Advanced Persistent Threats) σε παγκόσμιο επίπεδο. Χαρακτηριστικότερο παράδειγμα της καταστροφικής ευπάθειας αυτών των συστημάτων αποτελεί η παραβίαση της γέφυρας του **Ronin Network**, η οποία οδήγησε σε απώλεια 625 εκατομμυρίων δολαρίων. Η δομική αδυναμία αυτού του μοντέλου έγκειται στο γεγονός ότι, εάν το έξυπνο συμβόλαιο-θησαυροφυλάκιο στο δίκτυο προέλευσης παραβιαστεί και τα πραγματικά νομίσματα κλαπούν, τα Wrapped Tokens στο δίκτυο προορισμού χάνουν αυτομάτως το αντίκρισμά τους (collateral backing) και η αξία τους μηδενίζεται ακαριαία, προκαλώντας συστημικό σοκ στις αποκεντρωμένες αγορές.

6.5.2 Μοντέλα Επαλήθευσης (Verification Models) και Μηχανισμοί Ασφαλείας

Η αξιοπιστία και η ακεραιότητα μιας γέφυρας διαλειτουργικότητας δεν εξαρτάται από το περιβάλλον διεπαφής (UI), αλλά αποκλειστικά από τον κρυπτογραφικό μηχανισμό που χρησιμοποιείται για την πιστοποίηση των δεδομένων (Relayer/Oracle Model). Στη βιβλιογραφία, διακρίνονται τρία θεμελιώδη μοντέλα:

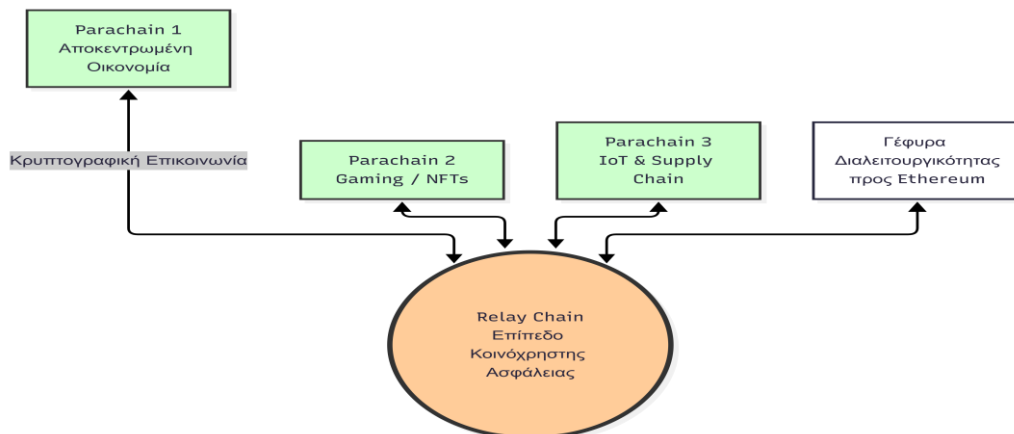
- **Εξωτερική Επαλήθευση (External Verification):** Η συγκεκριμένη αρχιτεκτονική βασίζεται στην ύπαρξη μιας ανεξάρτητης ομάδας ενδιάμεσων επικυρωτών (Third-party Oracles ή Multisig Wallets). Εάν η πλειοψηφία των επικυρωτών υπογράψει ψηφιακά (consensus thresholds) ότι επιβεβαίωσε την κατάθεση στο πρώτο δίκτυο, το δεύτερο δίκτυο εγκρίνει τη συναλλαγή. Ενώ αποτελεί την ταχύτερη και πιο εύκολα υλοποιήσιμη λύση, εισάγει ένα εξαιρετικά επικίνδυνο Σημείο Μοναδικής Αποτυχίας (Single Point of

Failure): θεωρείται κεντρικοποιημένο μοντέλο και είναι απόλυτα ευάλωτο. Εάν οι ιδιωτικοί κωδικοί της πλειοψηφίας των επικυρωτών υποκλαπούν (όπως συνέβη στο Ronin Hack), ολόκληρο το σύστημα καταρρέει.

- **Εγγενής Επαλήθευση (Native Verification - Light Clients):** Σε αυτό το μοντέλο, το δίκτυο προορισμού εκτελεί εντός του κώδικά του έναν ψηφιακό "Ελαφρύ Κόμβο" (Light Client) του δικτύου προέλευσης. Αυτό του επιτρέπει να επαληθεύει κρυπτογραφικά, χρησιμοποιώντας Αποδείξεις Merkle (Merkle Proofs), τις επικεφαλίδες (headers) των μπλοκ απευθείας, χωρίς καμία μεσολάβηση τρίτων (Trustless Execution). Αποτελεί την απόλυτη και πλέον ασφαλή μορφή διαλειτουργικότητας. Το συντριπτικό της μειονέκτημα, ωστόσο, έγκειται στο γεγονός ότι η εκτέλεση και συνεχής ενημέρωση ενός Light Client εντός ενός έξυπνου συμβολαίου (π.χ. στο δίκτυο του Ethereum) απαιτεί εξωφρενικά κόστη υπολογιστικού πόρου (Gas fees), καθιστώντας το μοντέλο οικονομικά απαγορευτικό για καθημερινή χρήση.
- **Τοπική Επαλήθευση (Local Verification - Atomic Swaps):** Σε αντίθεση με τις γέφυρες ρευστότητας, η Τοπική Επαλήθευση λειτουργεί αυστηρά μέσω Ατομικών Ανταλλαγών (Atomic Swaps / Hashed Timelock Contracts - HTLC). Δύο πρόσωπα ανταλλάσσουν άμεσα τα περιουσιακά τους στοιχεία σε διαφορετικά δίκτυα ταυτόχρονα. Αν η συναλλαγή δεν ολοκληρωθεί πλήρως και για τις δύο πλευρές εντός προκαθορισμένου χρόνου, ακυρώνεται αυτόματα και τα νομίσματα επιστρέφουν στους αρχικούς κατόχους, διασφαλίζοντας 100% προστασία χωρίς τη μεσολάβηση κεντρικών δεξαμενών ρευστότητας.

6.5.3 Οι Αρχιτεκτονικές του Επίπεδου 0 (Layer 0): Cosmos και Polkadot

Αντιλαμβανόμενη τους δομικούς περιορισμούς, τα ασύμμετρα σημεία μοναδικής αποτυχίας (Single Points of Failure) και τους εγγενείς κινδύνους των παραδοσιακών Γεφυρών (Cross-Chain Bridges) —οι οποίες, όπως αναλύθηκε, προστίθενται συνήθως εκ των υστέρων ως τεχνολογικά «μπαλώματα» πάνω σε ασύμβατες υποδομές— η βιομηχανία προχώρησε στο σχεδιασμό δικτύων «Επίπεδου 0» (Layer 0). Αντλώντας έμπνευση από το μοντέλο αναφοράς OSI των παραδοσιακών δικτύων υπολογιστών, τα δίκτυα αυτά σχεδιάστηκαν εξ αρχής (from the ground up) με έναν και μοναδικό, εξειδικευμένο σκοπό: την παροχή του υποκείμενου θεμελίου για την απρόσκοπτη, εγγενή διασύνδεση πολλαπλών, ανεξάρτητων Blockchains, δημιουργώντας οικοσυστήματα διαλειτουργικότητας στον πυρήνα τους.



Εικόνα 17: Τοπολογία Δικτύου Επίπεδου 0 (Layer 0) στην αρχιτεκτονική του Polkadot. Οι εξειδικευμένες αλυσίδες (Parachains) αντλούν κοινόχρηστη ασφάλεια από την Κεντρική Αλυσίδα Αναμετάδοσης (Relay Chain).

Το **Cosmos** (το οποίο συχνά αναφέρεται στη διεθνή βιβλιογραφία ως το "Διαδίκτυο των Blockchains" - Internet of Blockchains) υιοθετεί μια τοπολογία «Κεντρικού Κόμβου και Ζωνών» (Hub and Zones). Στο οικοσύστημα αυτό, κάθε «Ζώνη» αποτελεί ένα απολύτως ανεξάρτητο, κυρίαρχο (sovereign) και αυτόνομο Blockchain, το οποίο κατασκευάζεται συνήθως μέσω του αρθρωτού πλαισίου ανάπτυξης Cosmos SDK. Η κρίσιμη διαφορά του Cosmos έγκειται στο γεγονός ότι κάθε Ζώνη διατηρεί πλήρη έλεγχο πάνω στην ασφάλειά της, διαθέτοντας το δικό της

ξεχωριστό σύνολο επικυρωτών (validators) και βασιζόμενη στον πανίσχυρο, ντετερμινιστικό μηχανισμό συναίνεσης **Tendermint BFT** (Byzantine Fault Tolerance).

Η ριζοσπαστική καινοτομία του δικτύου εντοπίζεται στο **Πρωτόκολλο Δια-Αλυσιδικής Επικοινωνίας (IBC - Inter-Blockchain Communication)**, το οποίο λειτουργεί ως το αντίστοιχο πρωτόκολλο TCP/IP για το Web3. Μέσω του IBC, οι κυρίαρχες Ζώνες δεν ανταλλάσσουν νομίσματα μέσω κεντρικών δεξαμενών, αλλά ανταλλάσσουν κρυπτογραφικά επαληθεύσιμα πακέτα δεδομένων, διαβάζοντας η μία την κατάσταση (state) της άλλης μέσω ελαφρών πελατών (Light Clients) που τρέχουν εντός των συμβολαίων τους. Αυτή η αρχιτεκτονική επιτυγχάνει **Άμεση Οριστικότητα (Instant Finality)** στη μεταφορά περιουσιακών στοιχείων και ελαχιστοποιεί τον κίνδυνο υποκλοπής μέσω κακόβουλων αναμεταδοτών (Relayers), καθώς η εμπιστοσύνη τοποθετείται στα ίδια τα μαθηματικά της συναίνεσης και όχι σε κάποιον μεσάζοντα.

Στον αντίποδα του μοντέλου της πλήρους αποκέντρωσης και κυριαρχίας του Cosmos, το **Polkadot** εισάγει μια ριζοσπαστική αρχιτεκτονική προσέγγιση «Ετερογενούς Κατακερματισμού» (Heterogeneous Sharding), η οποία επικεντρώνεται στο δόγμα της **«Κοινόχρηστης Ασφάλειας» (Shared Security)**.

Στο κλασικό μοντέλο ανάπτυξης, κάθε νέο, εξειδικευμένο Blockchain οφείλει να αναζητήσει, να προσελκύσει και να χρηματοδοτήσει (μέσω πληθωρισμού του νομίσματός του) τους δικούς του ανεξάρτητους κόμβους για να εξασφαλίσει το δίκτυο. Αυτό αφήνει τις νεοφυείς αλυσίδες εξαιρετικά ευάλωτες σε κυβερνοεπιθέσεις του 51% (51% Attacks), λόγω της χαμηλής αρχικής τους κεφαλαιοποίησης (Market Cap). Το Polkadot επιλύει οριστικά αυτό το οικονομικό και τεχνολογικό πρόβλημα, καταργώντας πλήρως τη διαδικασία της συναίνεσης σε επίπεδο αλυσίδας-πελάτη. Αντίθετα, όλες οι Παράλληλες Αλυσίδες (**Parachains**) επικεντρώνονται αποκλειστικά στην εκτέλεση εξειδικευμένων εφαρμογών (π.χ. DeFi, Gaming, IoT) και συνδέονται κεντρικά σε μια κεντρική «ραχοκοκαλιά», την Αλυσίδα Αναμετάδοσης (**Relay Chain**).

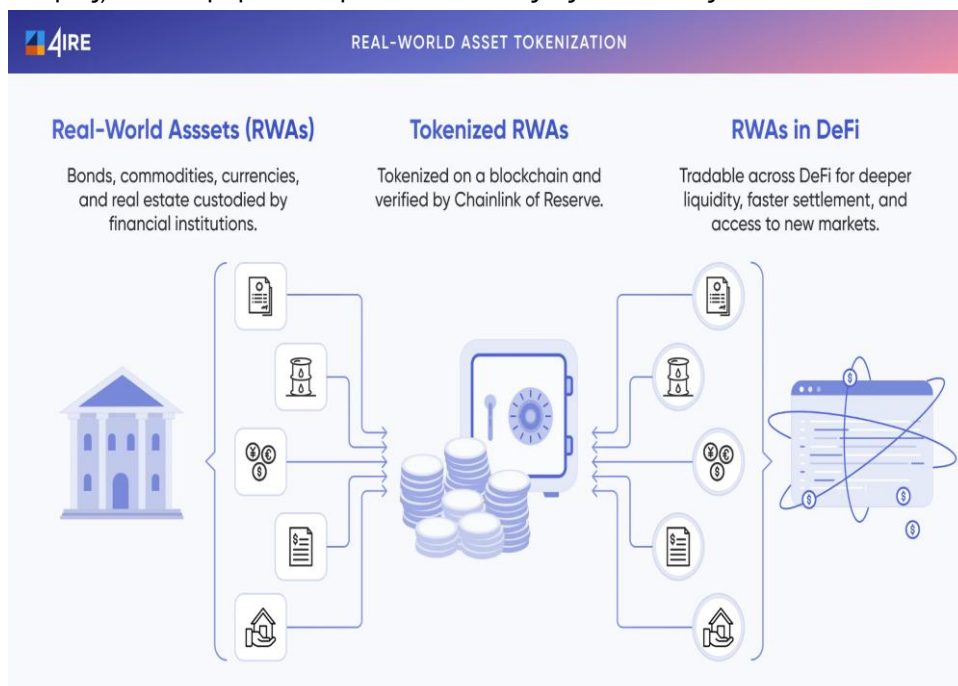
Το πλέον αξιοσημείωτο στοιχείο αυτής της αρχιτεκτονικής είναι ότι η ίδια η Relay Chain είναι απολύτως "αδρανής" σε επίπεδο προγραμματισμού εφαρμογών: δεν διαθέτει την ικανότητα εκτέλεσης έξυπνων συμβολαίων (smart contracts). Η μοναδική της, εξόχως κρίσιμη λειτουργία είναι η ενορχήστρωση του συστήματος μέσω ενός μοντέλου Εξουσιοδοτημένης Απόδειξης Συμμετοχής (Nominated Proof of Stake - NPoS). Παρέχει, με αυτόν τον τρόπο, «τυφλά» και απρόσκοπτα παγκόσμια κρυπτογραφική ασφάλεια και ενιαία συναίνεση (μέσω των αλγορίθμων BABE & GRANDPA) σε όλες τις Parachains ταυτόχρονα. Το μοντέλο της κοινόχρηστης ασφάλειας εξισώνει ουσιαστικά το επίπεδο προστασίας: ακόμα και το πιο μικρό, νεοσύστατο αποκεντρωμένο δίκτυο που συνδέεται στο οικοσύστημα, κληρονομεί ακαριαία την ίδια ακριβώς οικονομική και κρυπτογραφική ασφάλεια δισεκατομμυρίων δολαρίων με εκείνη του κεντρικού πυρήνα του Polkadot.

7. Τοκενοποίηση, Ψηφιακή Ταυτότητα και Θεσμικό Πλαίσιο MiCA

Η ωρίμανση του οικοσυστήματος Blockchain σηματοδοτεί τη μετάβαση από τα αμιγώς ψηφιακά περιουσιακά στοιχεία (όπως το Bitcoin) στην ενσωμάτωση της τεχνολογίας με την παραδοσιακή οικονομία. Το επόμενο σύνορο της αποκεντρωμένης πληροφορικής είναι η ψηφιοποίηση των τίτλων ιδιοκτησίας του φυσικού κόσμου και η δημιουργία ενός ασφαλούς ρυθμιστικού πλαισίου.

7.1 Τοκενοποίηση Πραγματικών Περιουσιακών Στοιχείων (RWA)

Η τοκενοποίηση (Tokenization) ορίζεται στο πλαίσιο της σύγχρονης χρηματοοικονομικής μηχανικής ως η διαδικασία ψηφιακής αναπαράστασης δικαιωμάτων ιδιοκτησίας, υλικών ή άυλων περιουσιακών στοιχείων (Real World Assets - RWA), σε ένα καταναμημένο καθολικό (Distributed Ledger). Η διαδικασία αυτή δεν συνιστά απλώς την απλή εγγραφή ή ψηφιοποίηση δεδομένων σε μια παραδοσιακή, κεντρική βάση, αλλά σηματοδοτεί τη δημιουργία ενός πλήρως προγραμματιζόμενου «έξυπνου τίτλου» (programmable asset). Αυτός ο τίτλος, μέσω της ενσωμάτωσης λογικής Έξυπνων Συμβολαίων (Smart Contracts), αλληλεπιδρά αυτόματα με το ευρύτερο αποκεντρωμένο χρηματοπιστωτικό σύστημα (DeFi). Το σημαντικότερο πλεονέκτημα αυτής της εξέλιξης είναι η απελευθέρωση πρωτοφανούς ρευστότητας σε παραδοσιακά «δυσκίνητες» και μη ρευστοποιήσιμες αγορές (illiquid markets), όπως το real estate, τα έργα τέχνης, τα ιδιωτικά επενδυτικά κεφάλαια (private equity) ή τα εταιρικά ομόλογα. Μέσω της κλασματικής ιδιοκτησίας (fractional ownership), ένα ακίνητο τεράστιας αξίας ή ένα θεσμικό ομόλογο μπορεί να διαιρεθεί σε χιλιάδες ψηφιακά μερίδια, εκδημοκρατίζοντας την πρόσβαση σε μικροεπενδυτές (retail investors) και καταργώντας το λεγόμενο "illiquidity premium" (ασφάλιστρο μη-ρευστότητας) που επιβαρύνει παραδοσιακά αυτές τις επενδύσεις..



Εικόνα 18: Τα στάδια ψηφιοποίησης και τοκενοποίησης Πραγματικών Περιουσιακών Στοιχείων (RWA) και η διασύνδεσή τους με τα αποκεντρωμένα δίκτυα.

Σε επίπεδο αρχιτεκτονικής, διαχείρισης κινδύνου και νομικής υπόστασης, η σύγχρονη ακαδημαϊκή κοινότητα και οι ρυθμιστικές αρχές διακρίνουν τα RWA σε δύο θεμελιώδεις και διακριτές κατηγορίες:

- **Μη-Εγγενή (Non-Native RWAs ή Off-chain Assets):** Πρόκειται για περιουσιακά στοιχεία τα οποία προϋπάρχουν και υφίστανται στον φυσικό κόσμο ή σε παραδοσιακά, κεντρικά μητρώα (π.χ. ακίνητα, μετοχές παραδοσιακών χρηματιστηρίων, ράβδοι χρυσού, εμπορεύματα). Σε αυτή την περίπτωση, το παραγόμενο κρυπτογραφικό token (συχνά

βασισμένο σε εξειδικευμένα πρότυπα ασφαλείας όπως το ERC-3643 για Security Tokens) λειτουργεί αποκλειστικά ως το «ψηφιακό είδωλο» (digital twin) του υποκείμενου στοιχείου. Ο κρισιμότερος κίνδυνος σε αυτή την κατηγορία είναι το λεγόμενο Πρόβλημα του Μαντείου στον φυσικό κόσμο (Physical Oracle Problem). Η αξία του token εξαρτάται απόλυτα από την εμπιστοσύνη σε τρίτους, κεντρικούς θεματοφύλακες (custodians) και από τη νομική ικανότητα επιβολής (legal enforceability) της σύνδεσης μεταξύ του ψηφιακού τίτλου στο Blockchain και του φυσικού αντικειμένου στο θησαυροφυλάκιο. Συνήθως, για να γεφυρωθεί αυτό το νομικό χάσμα, απαιτείται η δημιουργία Νομικών Οχημάτων Ειδικού Σκοπού (Special Purpose Vehicles - SPVs) τα οποία κατέχουν νόμιμα το φυσικό στοιχείο, με τα tokens να λειτουργούν ως ψηφιακές μετοχές του SPV.

- **Εγγενή (Native RWAs ή On-chain Assets):** Πρόκειται για περιουσιακά στοιχεία που "γεννιούνται" και εκδίδονται απευθείας εντός του Blockchain, χωρίς να υπάρχει κανένα φυσικό αντίστοιχο σε παραδοσιακά χάρτινα ή ηλεκτρονικά αποθετήρια. Ένα χαρακτηριστικό παράδειγμα αποτελούν τα ψηφιακά ομόλογα που εκδίδονται από μεγάλες τράπεζες (όπως τα ψηφιακά ομόλογα της Ευρωπαϊκής Τράπεζας Επενδύσεων) απευθείας σε δημόσια δίκτυα, ή τα αμιγώς ψηφιακά παράγωγα. Εδώ, το token δεν αναπαριστά το περιουσιακό στοιχείο· το token είναι το ίδιο το περιουσιακό στοιχείο. Η εγγενής τοκενοποίηση εξαλείφει πλήρως την ανάγκη για ενδιάμεσους εκκαθαριστικούς οίκους (Clearinghouses) και Κεντρικά Αποθετήρια Αξιών (CSDs). Η εκκαθάριση της συναλλαγής και η μεταβίβαση της κυριότητας πραγματοποιείται ακαριαία, ταυτόχρονα με την πληρωμή (Atomic Settlement - DVP). Αυτό μειώνει τον παραδοσιακό χρόνο διακανονισμού από δύο εργάσιμες ημέρες (T+2) σε σχεδόν μηδενικό χρόνο (T+0), εξαλείφοντας ριζικά τον πιστωτικό κίνδυνο αντισυμβαλλομένου (counterparty risk) κατά τη διάρκεια της συναλλαγής.

7.1.1 Τεχνικά Πρότυπα Ασφαλείας: ERC-1400 και ERC-3643

Ενώ τα συμβατικά πρότυπα τοκενοποίησης (όπως το ευρέως διαδεδομένο ERC-20) σχεδιάστηκαν ιστορικά με γνώμονα την ελεύθερη, χωρίς άδεια (permissionless) μεταβιβασιμότητα και την πλήρη ψευδωνυμία των συμμετεχόντων, τα Πραγματικά Περιουσιακά Στοιχεία (RWAs) — και ειδικότερα οι Τοκενοποιημένοι Τίτλοι (Security Tokens)— υπόκεινται σε αυστηρότατα διεθνή κανονιστικά και νομικά πλαίσια. Η νομοθεσία περί κινητών αξιών απαιτεί την υποχρεωτική εφαρμογή ελέγχων Γνώσης του Πελάτη (KYC - Know Your Customer) και Καταπολέμησης της Νομιμοποίησης Εσόδων από Παράνομες Δραστηριότητες (AML - Anti-Money Laundering). Για τη γεφύρωση αυτού του ρυθμιστικού χάσματος μεταξύ της παραδοσιακής χρηματοοικονομικής (TradFi) και του Web3, η κοινότητα ανέπτυξε εξειδικευμένα, αδειοδοτημένα (permissioned) πρότυπα έξυπνων συμβολαίων.

Το πρότυπο ERC-1400 (The Security Token Standard) δημιουργήθηκε για να καλύψει την πολυπλοκότητα των παραδοσιακών χρηματοοικονομικών μέσων. Εισάγει την κρίσιμη έννοια των «Τμημάτων» (Partitions / Tranches). Αυτή η αρχιτεκτονική επιτρέπει στο ίδιο ακριβώς token να αντιπροσωπεύει ταυτόχρονα διαφορετικές νομικές καταστάσεις (states) και διακριτά δικαιώματα. Για παράδειγμα, ένα μερίδιο μπορεί να ταξινομηθεί σε κοινές μετοχές με δικαίωμα ψήφου, ενώ ένα άλλο τμήμα του ίδιου token να λειτουργεί ως προνομιούχος μετοχή χωρίς δικαίωμα ψήφου αλλά με προτεραιότητα στη διανομή μερίσματος. Επιπλέον, το ERC-1400 υποστηρίζει εγγενώς τον «Έλεγχο Διαχειριστή» (Operator Control). Σε αντίθεση με την παραδοσιακή αποκεντρωμένη αρχή "code is law" (όπου η απώλεια κλειδιών σημαίνει οριστική απώλεια των κεφαλαίων), ο Έλεγχος Διαχειριστή παρέχει την τεχνική ικανότητα σε μια νομικά εξουσιοδοτημένη οντότητα (π.χ. έναν εγκεκριμένο θεματοφύλακα) να ανακτήσει ή να εκτελέσει εξαναγκαστική μεταφορά (forced transfer) των tokens, στην περίπτωση που υπάρξει κλοπή, απώλεια κωδικών πρόσβασης ή ρητή δικαστική απόφαση (court order).

Συμπληρωματικά, το ERC-3643 (γνωστό παλαιότερα ως T-Rex Protocol - Token for Regulated EXchanges) εστιάζει αποκλειστικά στη διαχείριση της ψηφιακής ταυτότητας και την αυτοματοποιημένη επιβολή της συμμόρφωσης. Το εν λόγω πρότυπο αλληλεπιδρά άμεσα με Αποκεντρωμένα Μητρώα Ταυτότητας (όπως το σύστημα ONCHAINID). Προτού εκτελεστεί οποιαδήποτε συνάρτηση μεταβίβασης (transfer()), το έξυπνο συμβόλαιο ελέγχει δυναμικά και σε πραγματικό χρόνο πολλαπλές παραμέτρους. Αποτρέπει τεχνολογικά τη μεταφορά του token εάν ο παραλήπτης δεν περιλαμβάνεται σε μια αυστηρή ψηφιακή "Λευκή Λίστα" (Whitelist), εάν δεν

έχει ολοκληρώσει επιτυχώς την κρυπτογραφική διαδικασία ταυτοποίησης (Verifiable Credentials), εάν προέρχεται από γεωγραφική δικαιοδοσία στην οποία έχουν επιβληθεί κυρώσεις (Sanctioned Jurisdictions), ή εάν δεν έχει παρέλθει η νομικά υποχρεωτική περίοδος διακράτησης (Lock-up period). Οι μη συμβατές συναλλαγές δεν ακυρώνονται απλώς εκ των υστέρων, αλλά απορρίπτονται προληπτικά στο χαμηλότερο επίπεδο του πρωτοκόλλου (reverted transactions), εκμηδενίζοντας τον κίνδυνο ρυθμιστικών παραβάσεων.

7.1.2 Διαφάνεια Αποθεματικών και Proof of Reserve

Η θεμελιώδης αρχιτεκτονική αδυναμία των Μη-Εγγενών RWAs (όπως τα stablecoins που υποστηρίζονται από παραστατικό χρήμα ή τα τοκενοποιημένα αποθέματα χρυσού) συνοψίζεται στο λεγόμενο Πρόβλημα του Μαντείου (The Oracle Problem). Καθώς το Blockchain αποτελεί ένα κλειστό, ντετερμινιστικό σύστημα, αδυνατεί να γνωρίζει ή να επαληθεύσει εάν το φυσικό περιουσιακό στοιχείο στον πραγματικό κόσμο υφίσταται όντως, εάν έχει κλαπεί, ή εάν έχει χρησιμοποιηθεί δόλια ως εγγύηση (collateral) πολλαπλές φορές σε διαφορετικά πιστωτικά ιδρύματα. Η αξιοπιστία ενός RWA εξαρτάται συνεπώς, σε απόλυτο βαθμό, από τη διαρκή και κρυπτογραφικά επαληθεύσιμη απόδειξη της ύπαρξης των υποκείμενων φυσικών αποθεματικών (off-chain assets).

Για την επίλυση αυτού του κρίσιμου συστημικού κινδύνου, η βιομηχανία ενσωματώνει Αποκεντρωμένα Δίκτυα Χρησμών (Decentralized Oracle Networks), με χαρακτηριστικότερο και πλέον αξιόπιστο παράδειγμα το πρωτόκολλο Proof of Reserve (PoR) (όπως υλοποιείται από το δίκτυο Chainlink). Μέσω αυτού του συστήματος, ανεξάρτητες ελεγκτικές εταιρείες παγκοσμίου βεληνεκούς (audit firms) και θεματοφύλακες παρακολουθούν συνεχώς τα υπόλοιπα των παραδοσιακών τραπεζικών λογαριασμών ή των φυσικών θησαυροφυλακίων. Τα δεδομένα αυτά κρυπτογραφούνται και μεταδίδονται (broadcast) αδιάκοπα στην αλυσίδα, διασφαλίζοντας 24/7 διαφάνεια.

Το σύστημα Proof of Reserve λειτουργεί ως μια δυναμική, αυτοματοποιημένη γέφυρα εμπιστοσύνης. Τα έξυπνα συμβόλαια που εκδίδουν τα RWAs είναι προγραμματισμένα να ελέγχουν αυτή τη συνεχή ροή δεδομένων πριν από κάθε νέα έκδοση νομισμάτων. Εάν, για οποιονδήποτε λόγο (όπως λογιστικό σφάλμα, απάτη ή κατάσχεση), η ροή πληροφοριών υποδείξει ότι η συνολική ψηφιακή προσφορά των tokens ετοιμάζεται να ξεπεράσει την αξία του επαληθευμένου φυσικού αποθέματος —δηλαδή το σύστημα απειλείται να περιέλθει σε κατάσταση υπο-εξασφάλισης (under-collateralization)— ο κώδικας του έξυπνου συμβολαίου ενεργοποιεί αυτόματα και αμετάκλητα αυστηρές δικλίδες ασφαλείας (Circuit Breakers). Αυτός ο μηχανισμός «παγώνει» (pauses) ακαριαία τη συνάρτηση παραγωγής (mint()), αποτρέποντας με μαθηματική βεβαιότητα την έκδοση ακάλυπτων ψηφιακών τίτλων. Με αυτόν τον τρόπο, το αποκεντρωμένο οικοσύστημα θωρακίζεται έναντι του συστημικού κινδύνου μετάδοσης (systemic contagion) και του "Bank Run", φαινόμενα που έχουν οδηγήσει ιστορικά σε καταρρεύσεις της παραδοσιακής τραπεζικής.

7.2 Το Ευρωπαϊκό Ρυθμιστικό Πλαίσιο MiCA και η Κανονιστική Συμμόρφωση

Η ψήφιση του Κανονισμού 2023/1114 για τις αγορές κρυπτοστοιχείων, γνωστού ως MiCA (Markets in Crypto-Assets), από την Ευρωπαϊκή Ένωση, προσφέρει νομική σαφήνεια και αυστηρούς κανόνες λειτουργίας, στοχεύοντας στην προστασία των καταναλωτών από απάτες και την ενίσχυση της καινοτομίας των θεσμικών επενδυτών.

Ο Κανονισμός ταξινομεί τα κρυπτοστοιχεία σε τρεις διακριτές κατηγορίες:

1. **Μάρκες Ηλεκτρονικού Χρήματος (E-Money Tokens - EMTs):** Αποτελούν νομίσματα σταθερής ισοτιμίας (Stablecoins) που συνδέονται με ένα μόνο επίσημο νόμισμα (π.χ. Ευρώ ή Δολάριο). Μπορούν να εκδίδονται μόνο από Πιστωτικά Ιδρύματα ή Ιδρύματα Ηλεκτρονικού Χρήματος. Ο εκδότης οφείλει να διατηρεί αποθεματικά 1:1 σε μετρητά, εξασφαλίζοντας το νομικό δικαίωμα εξαργύρωσης στην ονομαστική αξία ανά πάσα στιγμή.
2. **Μάρκες Αναφοράς σε Περιουσιακά Στοιχεία (Asset-Referenced Tokens - ARTs):** Πρόκειται για νομίσματα που η αξία τους βασίζεται σε ένα καλάθι νομισμάτων ή

εμπορευμάτων. Λόγω του συστημικού κινδύνου που εγκυμονούν για τη νομισματική κυριαρχία του Ευρώ, υπόκεινται σε αυστηρά όρια ημερήσιων συναλλαγών, τα οποία αν παραβιαστούν, η Ευρωπαϊκή Κεντρική Τράπεζα (ΕΚΤ) δύναται να διακόψει την κυκλοφορία τους.

3. **Μάρκες Χρησιμότητας (Utility Tokens):** Πρόκειται για λοιπά κρυπτονομίσματα που εξυπηρετούν σκοπούς εντός πλατφορμών. Επιβάλλεται η δημοσίευση εγκεκριμένης Λευκής Βίβλου (Whitepaper) με σαφή περιγραφή των κινδύνων και της τεχνολογίας.

Οι ενδιαμέσοι πάροχοι (Ανταλλακτήρια, Θεματοφύλακες), οριζόμενοι ως CASPs (Crypto-Asset Service Providers), επωμίζονται βαρύτατες υποχρεώσεις. Απαιτείται φυσική έδρα στην ΕΕ, αυστηρός διαχωρισμός των κεφαλαίων της εταιρείας από τα κεφάλαια των πελατών (Segregation of Funds) για την αποτροπή περιπτώσεων υπεξαίρεσης, και φέρουν απόλυτη νομική ευθύνη αποζημίωσης σε περίπτωση απώλειας κρυπτοστοιχείων λόγω κυβερνοεπίθεσης (hack) στα συστήματά τους. Επιπλέον, υπόκεινται στον "Ταξιδιωτικό Κανόνα" (Travel Rule - TFR), ο οποίος υποχρεώνει τη διαβίβαση των προσωπικών στοιχείων αποστολέα και παραλήπτη σε κάθε μεταφορά κεφαλαίων για την καταπολέμηση της νομιμοποίησης εσόδων (AML).

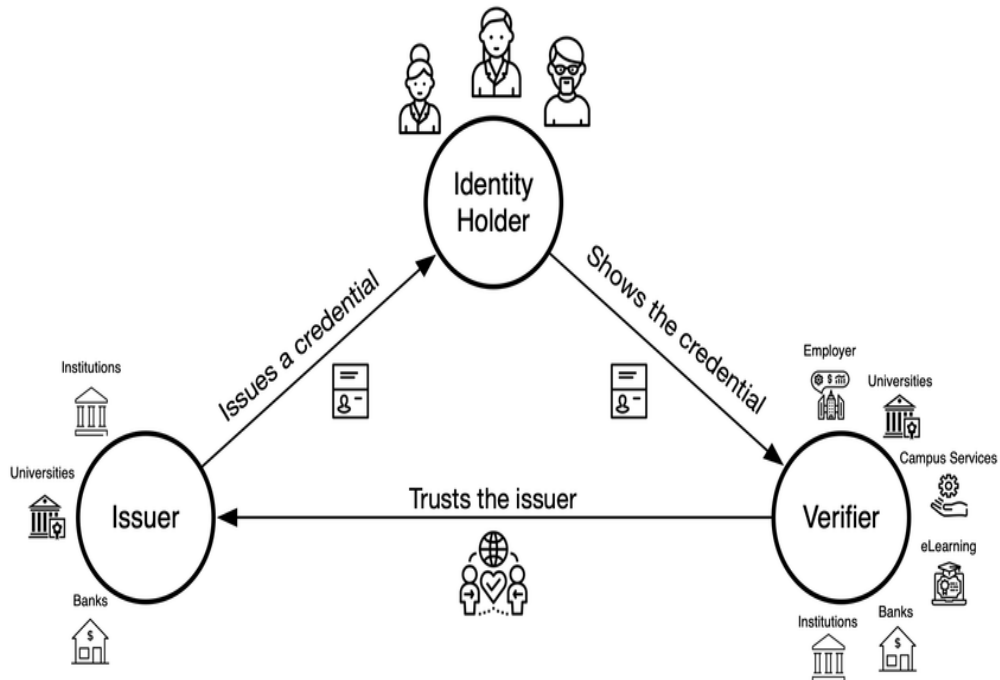
7.3 Ψηφιακά Νομίσματα Κεντρικών Τραπεζών (CBDCs)

Τα CBDC (Central Bank Digital Currencies) αποτελούν την ψηφιακή εκδοχή του κρατικού χρήματος, η οποία διατίθεται απευθείας στο ευρύ κοινό. Για την αποτροπή της αποσταθεροποίησης του συστήματος των εμπορικών τραπεζών (Bank Runs), υιοθετείται το Υβριδικό Μοντέλο Δύο Επιπέδων (Two-Tier Model). Η Κεντρική Τράπεζα διαχειρίζεται το κεντρικό καθολικό χονδρικής (Wholesale Ledger) και εκδίδει το νόμισμα, ενώ οι εμπορικές τράπεζες ή οι πάροχοι πληρωμών (PSPs) αναλαμβάνουν τη διανομή, την ταυτοποίηση των πελατών (KYC) και τη λειτουργία των ψηφιακών πορτοφολιών λιανικής, διατηρώντας τα προσωπικά δεδομένα των πολιτών μακριά από τον άμεσο έλεγχο του κράτους.

Αν και πειράματα όπως το Project Hamilton έχουν αποδείξει ότι οι κεντρικές βάσεις δεδομένων είναι επαρκείς για την ταχύτατη διεκπεραίωση πληρωμών, πολλές κεντρικές τράπεζες προσανατολίζονται στην υιοθέτηση κατανεμημένων καθολικών (συνήθως Permissioned DLTs) για να εκμεταλλευτούν την "Ατομικότητα" (Atomicity) και τα Έξυπνα Συμβόλαια. Στον τομέα των διασυννοριακών πληρωμών, το Project mBridge φιλοδοξεί να υποκαταστήσει το αργό δίκτυο SWIFT, επιτρέποντας άμεσες Peer-to-Peer συναλλαγές μεταξύ κεντρικών τραπεζών μέσω ενός κοινού DLT. Για τη διασφάλιση της ιδιωτικότητας των συναλλαγών και των δυνατοτήτων πληρωμής εκτός σύνδεσης (offline payments), αξιοποιούνται κρυπτογραφικές αποδείξεις Zero-Knowledge Proofs και ειδικά τσιπ ασφαλείας (Secure Elements - NFC) σε κινητά τηλέφωνα.

7.4 Αυτοκυρίαρχη Ταυτότητα (Self-Sovereign Identity - SSI)

Το υφιστάμενο ψηφιακό μοντέλο διαχείρισης ταυτότητας είναι κεντριοποιημένο, καθώς η πρόσβαση των χρηστών εξαρτάται από μεγάλους παρόχους (Identity Providers). Το Web3 προτείνει την Αυτοκυρίαρχη Ταυτότητα (SSI), όπου ο χρήστης καθίσταται ο αποκλειστικός ιδιοκτήτης και διαχειριστής των διαπιστευτηρίων του.



Εικόνα 19: Το «Τρίγωνο Εμπιστοσύνης» της Αυτοκυρίαρχης Ταυτότητας (SSI) και η αποκεντρωμένη ανταλλαγή Επαληθεύσιμων Διαπιστευτηρίων.

Η τεχνολογική βάση της SSI στηρίζεται στα Αποκεντρωμένα Αναγνωριστικά (Decentralized Identifiers - DIDs) και τα Επαληθεύσιμα Διαπιστευτήρια (Verifiable Credentials - VCs), σύμφωνα με τα πρότυπα του οργανισμού W3C. Η διαδικασία λειτουργεί μέσω του «Τρίγωνου Εμπιστοσύνης»:

1. **Ο Εκδότης (Issuer):** Υπογράφει ψηφιακά ένα πιστοποιητικό (π.χ. ένα πανεπιστήμιο που εκδίδει πτυχίο).
2. **Ο Κάτοχος (Holder):** Αποθηκεύει το VC τοπικά στο προσωπικό του ψηφιακό πορτοφόλι.
3. **Ο Επαληθευτής (Verifier):** Ελέγχει την κρυπτογραφική υπογραφή του Εκδότη μέσω του Blockchain, αποκτώντας μαθηματική βεβαιότητα για την εγκυρότητα του εγγράφου, χωρίς να χρειάζεται να επικοινωνήσει με την αρχή έκδοσης.

Μέσω της τεχνολογίας Zero-Knowledge (zk-KYC), ο χρήστης μπορεί να αποδείξει στον Επαληθευτή μια ιδιότητα (π.χ. Επιλεκτική Αποκάλυψη - Selective Disclosure ότι είναι άνω των 18 ετών), χωρίς να αποκαλύψει την πραγματική ημερομηνία γέννησης ή την ταυτότητά του, ενισχύοντας θεαματικά την ιδιωτικότητα. Περαιτέρω, έχουν προταθεί και τα Soulbound Tokens (SBTs), τα οποία είναι μη-μεταβιβάσιμα NFTs που προσδένονται μόνιμα στο πορτοφόλι του χρήστη, λειτουργώντας ως ψηφιακά πιστοποιητικά δεξιοτήτων, ιατρικών φακέλων ή ως εργαλεία οικοδόμησης πιστοληπτικής φήμης (on-chain credit score). Στον αντίποδα, πρωτοβουλίες όπως το Worldcoin (βασισμένες σε σάρωση ίριδας/βιομετρία για την απόδειξη του "Proof of Personhood") εγείρουν σοβαρές ανησυχίες δυστοπικής παρακολούθησης.

7.5 Αποκεντρωμένα Δίκτυα Φυσικών Υποδομών (DePIN)

Μια από τις πλέον υποσχόμενες εφαρμογές της κρυπτο-οικονομίας είναι τα DePIN (Decentralized Physical Infrastructure Networks). Αποτελούν δίκτυα τηλεπικοινωνιών, υπολογιστικής ισχύος ή

αποθήκευσης που κατασκευάζονται και συντηρούνται μέσω συμμετοχικής χρηματοδότησης και εργασίας από τους ίδιους τους χρήστες (Crowdsourcing), ανταγωνιζόμενα τις παραδοσιακές κεντρικές υποδομές Cloud με κλάσμα του κόστους (Capex).

Τα δίκτυα DePIN διακρίνονται σε δύο μεγάλες υποκατηγορίες:

- **Δίκτυα Φυσικών Πόρων (Physical Resource Networks - PRNs):** Η λειτουργία και η ανταμοιβή τους εξαρτάται άμεσα από τη γεωγραφική τοποθεσία της συσκευής. Ένα παράδειγμα είναι τα δίκτυα αποκεντρωμένης ασύρματης κάλυψης (όπως το Helium) ή τα δίκτυα χαρτογράφησης, όπου η τοποθέτηση του υλικού σε στρατηγικά σημεία είναι κρίσιμη για την αποδοτικότητα.
- **Δίκτυα Ψηφιακών Πόρων (Digital Resource Networks - DRNs):** Πόροι που δεν εξαρτώνται από τη γεωγραφία και είναι ελεύθερα ανταλλάξιμοι (fungible). Παραδείγματα αποτελούν τα δίκτυα διαμοιρασμού υπολογιστικής ισχύος καρτών γραφικών (GPUs) για εκπαίδευση μοντέλων Τεχνητής Νοημοσύνης (όπως το Render Network) ή τα αποκεντρωμένα συστήματα αποθήκευσης αρχείων (όπως το Filecoin).

Η ανάπτυξη αυτών των υποδομών βασίζεται στον οικονομικό κύκλο κινήτρων (DePIN Flywheel). Στα αρχικά στάδια του δικτύου, όπου η ζήτηση είναι ανύπαρκτη, οι χρήστες (Supply Side) επιδοτούνται με τα tokens του πρωτοκόλλου για να αναπτύξουν τον εξοπλισμό. Καθώς το δίκτυο μεγαλώνει, καθίσταται αξιόπιστο και προσελκύει επιχειρήσεις που πληρώνουν για τις υπηρεσίες. Αυτά τα έσοδα χρησιμοποιούνται συχνά για την επαναγορά και καταστροφή (Burn) των tokens, μειώνοντας την προσφορά, αυξάνοντας την τιμή τους και προσελκύοντας νέους παρόχους υλικού.

Για την επαλήθευση των εργασιών σε αυτά τα συστήματα εισάγονται εξειδικευμένοι μηχανισμοί συναίνεσης. Ο μηχανισμός Απόδειξης Κάλυψης (Proof of Coverage - PoC) χρησιμοποιεί κρυπτογραφημένα σήματα (beacons) μεταξύ γεωγραφικά γειτονικών συσκευών (witnesses) προκειμένου να επικυρώσει την πραγματική θέση ενός κόμβου, αποκλείοντας κακόβουλους χρήστες που προσπαθούν να ξεγελάσουν το σύστημα (spoofing). Αντίστοιχα, τα δίκτυα υπολογιστικής ισχύος χρησιμοποιούν συχνά Απόδειξεις Μηδενικής Γνώσης (Zero-Knowledge Verifiable Computing) ώστε ο πελάτης να είναι απόλυτα βέβαιος ότι η GPU εκτέλεσε σωστά τον περίπλοκο αλγόριθμο AI, χωρίς να χρειάζεται να επαναλάβει ο ίδιος τον υπολογισμό. Επειδή, τέλος, τα δεδομένα αυτών των συσκευών αποτελούν "Big Data", η επεξεργασία τους πραγματοποιείται εκτός αλυσίδας (Off-Chain), ενώ το Blockchain χρησιμοποιείται αποκλειστικά ως το τελικό επίπεδο εκκαθάρισης των πληρωμών και των αποδείξεων.

8. Η Οικονομία της Προσοχής: Memecoins, Συμπεριφορική Χρηματοοικονομική και Δυναμική των Αγορών

Η επισταμένη τεχνική επισκόπηση των κατανεμημένων υποδομών του Blockchain και των πρωτοκόλλων της Αποκεντρωμένης Χρηματοοικονομικής (DeFi) θα καθίστατο εννοιολογικά ατελής, εάν δεν εξετάζαμε ένα από τα πιο ιδιόζοντα και αμφιλεγόμενα φαινόμενα του χώρου: τα λεγόμενα «Memecoins». Πρόκειται για μια ιδιαίτερη κατηγορία ψηφιακών νομισμάτων η οποία, παρά την προφανή και συχνά εσκεμμένη έλλειψη εγγενούς τεχνολογικής χρησιμότητας (utility), κατορθώνει να συγκεντρώνει, να διακινεί και να δεσμεύει τεράστιο όγκο κεφαλαίων, απορροφώντας ταυτόχρονα ένα πρωτοφανές μερίδιο του κοινωνικού ενδιαφέροντος.

Σε πλήρη αντίθεση με τα θεμελιώδη ψηφιακά περιουσιακά στοιχεία, όπως το Bitcoin, ή τα προγραμματιζόμενα tokens υποδομής, όπως το Ethereum —τα οποία αντλούν την αξία τους από τη μαθηματικά διασφαλισμένη σπανιότητα, την αρχιτεκτονική ασφάλεια του δικτύου και τον ρόλο τους ως «καύσιμο» (gas) για την εκτέλεση πολύπλοκων υπολογισμών— τα memecoins εκπροσωπούν μια ριζικά εναλλακτική θεώρηση της αγοράς. Υπό το πρίσμα της Συμπεριφορικής Χρηματοοικονομικής (Behavioral Finance), η αποτίμησή τους δεν εδράζεται σε κανένα τεχνολογικό πλεονέκτημα, σε αναμενόμενες ταμειακές ροές (DCF) ή σε παραδοσιακά εταιρικά θεμελιώδη. Αντιθέτως, τροφοδοτείται αποκλειστικά από τη δυναμική της ψηφιακής κοινότητας, το φαινόμενο της αγέλης (herd mentality) και τους αδυσώπητους κανόνες της «Οικονομίας της Προσοχής» (Attention Economy). Στο οικοσύστημα αυτό, παρατηρούμε την απόλυτη χρηματιστικοποίηση της ανθρώπινης προσοχής (hyper-financialization), όπου το κοινωνικό κεφάλαιο (social capital) μιας διαδικτυακής τάσης μετατρέπεται ακαριαία σε άμεσα ρευστοποιήσιμη ψηφιακή αξία.

8.1 Ιστορική Αναδρομή: Από την Παρωδία στη Βιομηχανία Δισεκατομμυρίων

Η αφετηρία αυτής της κατηγορίας τοποθετείται ιστορικά στο 2013, με τη δημιουργία του Dogecoin (DOGE). Στην αρχική του σύλληψη, αναπτύχθηκε ως μια καλοπροαίρετη, χιουμοριστική σάτιρα απέναντι στην αλόγιστη κερδοσκοπία και την αυξανόμενη τεχνική πολυπλοκότητα του οικοσυστήματος του Bitcoin. Σε επίπεδο υποδομής, το Dogecoin αποτέλεσε έναν άμεσο διακλαδισμό (hard fork) του πηγαίου κώδικα του Litecoin. Διατήρησε τον αλγόριθμο συναίνεσης Απόδειξης Εργασίας (Proof of Work), αξιοποιώντας την κρυπτογραφική συνάρτηση κατακερματισμού Scrypt. Παρά την απουσία ανώτατου ορίου στην έκδοση νομισμάτων (ακολουθώντας ένα πληθωριστικό μοντέλο χωρίς hard cap) και τη μακροχρόνια στασιμότητα στην ανάπτυξη του κώδικά του, κατόρθωσε να δομήσει μια πολυπληθή και φανατική βάση χρηστών, αποδεικνύοντας πολύ νωρίς τη δύναμη του κοινοτικού φαινομένου (network effect).

Ωστόσο, η πραγματική τεχνολογική και οικονομική μετάλλαξη της αγοράς σημειώθηκε την περίοδο 2020-2021, με την εκρηκτική άνοδο του Shiba Inu (SHIB). Το συγκεκριμένο εγχείρημα εισήγαγε μια κρίσιμη αρχιτεκτονική διαφοροποίηση: δεν βασίστηκε στη χρονοβόρα δημιουργία ενός αυτόνομου δικτύου (Layer 1 Blockchain) με δικούς του κόμβους και εξορύκτες, αλλά εκδόθηκε απλώς ως ένα ψηφιακό token τυποποίησης ERC-20, "πατώντας" εξ ολοκλήρου πάνω στην υφιστάμενη υποδομή του Ethereum. Αυτή η αφαίρεση του δικτυακού επιπέδου υπήρξε καταλυτική. Απέδειξε στην πράξη ότι οποιοσδήποτε προγραμματιστής, γράφοντας ελάχιστες γραμμές κώδικα στη γλώσσα Solidity, μπορούσε να εκδώσει ένα ψηφιακό περιουσιακό στοιχείο και να του προσφέρει ακαριαία, παγκόσμια ρευστότητα συνδέοντάς το με Αποκεντρωμένα Ανταλλακτήρια (DEXs) όπως το Uniswap.

Φτάνοντας στις αρχές του 2024, το κέντρο βάρους της βιομηχανίας μετατοπίστηκε βίαια προς δικτυακές αρχιτεκτονικές υψηλής διαμετακομιστικής ικανότητας (high throughput) και εξαιρετικά χαμηλών τελών, με κυρίαρχο το δίκτυο του Solana. Η απουσία υπολογιστικής συμφόρησης και τα μηδαμινά τέλη (sub-cent fees) πυροδότησαν τη δημιουργία αυτοματοποιημένων πρωτοκόλλων έκδοσης (launchpads). Αυτές οι πλατφόρμες εκμηδένισαν πλήρως το τεχνικό εμπόδιο εισόδου, μετατρέποντας την παραγωγή νέων tokens σε μια πλήρως αυτοματοποιημένη, μαζική και σχεδόν μηδενικού κόστους διαδικασία, προσιτή ακόμα και σε χρήστες χωρίς καμία γνώση προγραμματισμού.

8.2 Τεχνολογική Υποδομή και Μηχανισμοί Ρευστότητας

Εξετάζοντας τα memecoins υπό το πρίσμα της επιστήμης των υπολογιστών, ερχόμαστε αντιμέτωποι με ένα έντονο τεχνολογικό παράδοξο. Παρότι τα ίδια τα περιουσιακά στοιχεία στερούνται, κατά κανόνα, οποιασδήποτε ουσιαστικής καινοτομίας (όντας συνήθως απλοϊκά συμβόλαια μεταβίβασης υπολοίπων), οι υποκείμενοι μηχανισμοί διακίνησης, αποτίμησης και ανταλλαγής τους στηρίζονται στις πλέον προηγμένες, περίπλοκες και κομψές μαθηματικές δομές της αποκεντρωμένης χρηματοοικονομικής μηχανικής.

8.2.1 Αυτοματοποιημένοι Ειδικοί Διαπραγματευτές (AMMs)

Στο παραδοσιακό χρηματοοικονομικό σύστημα, καθώς και στα Κεντρικοποιημένα Ανταλλακτήρια Κρυπτονομισμάτων (CEXs), η ένταξη ενός νέου περιουσιακού στοιχείου προς διαπραγμάτευση (listing) αποτελεί μια δυσκίνητη διαδικασία. Απαιτεί χρονοβόρες διοικητικές εγκρίσεις, αυστηρή κανονιστική συμμόρφωση (KYC/AML) και την καταβολή υπέρογκων τελών. Επιπρόσθετα, η ρευστότητα βασίζεται στο παραδοσιακό Κεντρικό Βιβλίο Εντολών (Central Limit Order Book - CLOB), το οποίο εξαρτάται από την αδιάλειπτη παρουσία θεσμικών Ειδικών Διαπραγματευτών (Market Makers). Το οικοσύστημα της Οικονομίας της Προσοχής προσπερνά εξ ολοκλήρου αυτούς τους περιορισμούς, αξιοποιώντας τη ριζοσπαστική αρχιτεκτονική των Αυτοματοποιημένων Ειδικών Διαπραγματευτών (Automated Market Makers - AMMs).

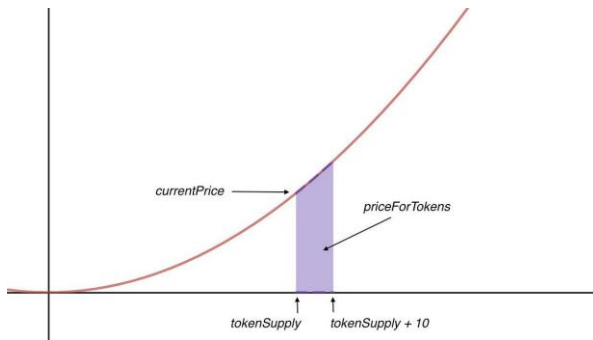
Η φύση των DEXs, όπως το Uniswap ή το Raydium, είναι εγγενώς ανοιχτή και «χωρίς άδεια» (permissionless). Ένας δημιουργός, παρακάμπτοντας κάθε κεντρικό ελεγκτή, μπορεί να συγκροτήσει μια Δεξαμενή Ρευστότητας (Liquidity Pool) αλληλεπιδρώντας απευθείας με το έξυπνο συμβόλαιο. Καταθέτει το νεοεκδοθέν memecoin μαζί με ένα εγγενές νόμισμα βάσης (όπως ETH ή SOL). Από εκείνη τη στιγμή, το έξυπνο συμβόλαιο αναλαμβάνει τον ρόλο του αδιάφθορου, μαθηματικού διαμεσολαβητή.

Η τιμολόγηση δεν εξαρτάται πλέον από το ταίριασμα ανθρώπινων εντολών αγοράς και πώλησης, αλλά ρυθμίζεται δυναμικά από έναν ντετερμινιστικό αλγόριθμο. Η πλέον καθιερωμένη υλοποίηση είναι το μοντέλο του Σταθερού Γινομένου (Constant Product Market Maker - CPMM), το οποίο εκφράζεται από τη θεμελιώδη εξίσωση:

$$x \cdot y = k$$

Όπου x και y αντιπροσωπεύουν τις συνολικές διαθέσιμες ποσότητες των δύο νομισμάτων εντός της δεξαμενής, και k αποτελεί τη σταθερά (invariant constant), η οποία διατηρείται αμετάβλητη μετά από κάθε συναλλαγή (εξαιρουμένων των τελών). Αυτός ο μηχανισμός σχηματίζει μια ασυμπτωτική υπερβολή. Εάν ένας χρήστης αγοράσει ποσότητα από το νόμισμα x (αφαιρώντας το από τη δεξαμενή), το συμβόλαιο απαιτεί την προσθήκη αυξημένης ποσότητας από το νόμισμα y , ώστε το γινόμενο k να παραμείνει σταθερό. Σε δεξαμενές με χαμηλή αρχική ρευστότητα (χαρακτηριστικό γνώρισμα των νέων εκδόσεων), αυτή η μαθηματική ιδιότητα προκαλεί ακραία «Ολίσθηση Τιμής» (Price Slippage), όπου ακόμη και μικρές εντολές αγοράς εκτινάσσουν την οριακή τιμή (marginal price) εκθετικά.

8.2.2 Καμπύλες Δέσμευσης (Bonding Curves)



Εικόνα 20: Μαθηματική αναπαράσταση μιας Καμπύλης Δέσμευσης (Bonding Curve) για τον αλγοριθμικό καθορισμό της τιμής βάσει προσφοράς και ζήτησης.

Μία από τις πλέον καινοτόμες και περίπλοκες μεθόδους αλγοριθμικής αποτίμησης και διανομής ψηφιακών στοιχείων, η οποία αποτέλεσε τον καταλύτη για τη μαζική έκρηξη των memecoins το 2024, είναι η αρχιτεκτονική των Καμπυλών Δέσμευσης (Bonding Curves). Στην παραδοσιακή αποκεντρωμένη χρηματοοικονομική (DeFi), η δημιουργία μιας αγοράς σε ένα ανταλλακτήριο προϋποθέτει ότι ο δημιουργός του νομίσματος διαθέτει και ρισκάρει το δικό του αρχικό κεφάλαιο (seed liquidity) για να χρηματοδοτήσει τη Δεξαμενή Ρευστότητας (Liquidity Pool). Αυτό το αρχιτεκτονικό εμπόδιο δημιουργούσε τον κίνδυνο των

«Επιθέσεων Αφαίρεσης Ρευστότητας» (Rug Pulls), όπου ο δημιουργός μπορούσε ανά πάσα στιγμή να αποσύρει τα κεφάλαια, αφήνοντας τους επενδυτές με νομίσματα μηδενικής αξίας.

Τα πρωτόκολλα που βασίζονται σε Καμπύλες Δέσμευσης εισάγουν ένα Συνεχές Μοντέλο Νομίσματος (Continuous Token Model). Σε αυτό το μοντέλο, το έξυπνο συμβόλαιο δεν λειτουργεί απλώς ως μεσάζοντας, αλλά ως ο μοναδικός εκδότης (minter) και αγοραστής (burner) του νομίσματος. Δεν υφίσταται προκαταβολική δημιουργία συνολικής προσφοράς (pre-mine) ούτε απαιτείται αρχική ρευστότητα από τον δημιουργό.

Η αποτίμηση του νομίσματος καθορίζεται αυστηρά αλγοριθμικά και αυξάνεται ντετερμινιστικά καθώς αυξάνεται η συνολική κυκλοφορούσα προσφορά. Η πιο συνήθης μαθηματική υλοποίηση ακολουθεί μια πολυωνυμική ή εκθετική συνάρτηση της μορφής:

$$P = c \cdot S^n$$

Όπου P είναι η τρέχουσα τιμή (Price) του νομίσματος, S είναι η συνολική κυκλοφορούσα προσφορά (Supply) τη δεδομένη χρονική στιγμή, c αποτελεί μια αυθαίρετη σταθερά καμπυλότητας που ορίζει το έξυπνο συμβόλαιο, και n εκφράζει τον εκθέτη (π.χ., εάν $n = 2$, η τιμή αυξάνεται τετραγωνικά σε σχέση με την προσφορά). Όταν ένας επενδυτής καταθέτει το νόμισμα βάσης (π.χ. SOL) στο συμβόλαιο, αυτό "κόβει" (mints) νέα νομίσματα και του τα αποδίδει, μετατοπίζοντας την τιμή προς τα πάνω στην καμπύλη. Αντιστρόφως, εάν πουλήσει, το συμβόλαιο καταστρέφει (burns) τα νομίσματα και του επιστρέφει το SOL, ρίχνοντας την τιμή.

Πρόσφατα, η εμφάνιση και η εκθετική υιοθέτηση εξειδικευμένων, αυτοματοποιημένων πλατφορμών έκδοσης (όπως το πρωτόκολλο Pump.fun στο δίκτυο του Solana) απλοποίησε περαιτέρω αυτή τη διαδικασία, εκδημοκρατίζοντας πλήρως την έκδοση νομισμάτων. Οι πλατφόρμες αυτές αξιοποιούν τις Καμπύλες Δέσμευσης για να προσφέρουν μια «Δίκαιη Εκκίνηση» (Fair Launch): κανείς—ούτε καν ο δημιουργός—δεν μπορεί να αποκτήσει νομίσματα δωρεάν· όλοι πρέπει να τα αγοράσουν βάσει της μαθηματικής καμπύλης.

Το πλέον εντυπωσιακό στοιχείο αυτής της αρχιτεκτονικής εντοπίζεται στον μηχανισμό Ατομικής Μετάβασης (Atomic Transition). Μόλις η κεφαλαιοποίηση του νομίσματος (ή η ρευστότητα σε SOL που έχει συσσωρευτεί στο έξυπνο συμβόλαιο) προσεγγίσει ένα αυστηρά προκαθορισμένο, ενσωματωμένο όριο (threshold / bonding curve cap), η καμπύλη «τερματίζει» τη λειτουργία της. Σε εκείνο το ακριβές χιλιοστό του δευτερολέπτου, το έξυπνο συμβόλαιο εκτελεί μια αμετάκλητη ακολουθία εντολών:

1. Σταματά την έκδοση νέων νομισμάτων.
2. Μεταφέρει όλη τη συσσωρευμένη ρευστότητα (το νόμισμα βάσης) και τα εναπομείναντα διαθέσιμα memecoins.
3. Δημιουργεί αυτόματα μια μόνιμη Δεξαμενή Ρευστότητας σε ένα κορυφαίο, παραδοσιακό Αποκεντρωμένο Ανταλλακτήριο (όπως το Raydium).
4. Κλειδώνει ή «καίει» (burns) οριστικά τα αποδεικτικά ιδιοκτησίας της ρευστότητας (LP

Αυτή η αυτοματοποιημένη διαδικασία διασφαλίζει την ανεμπόδιστη, διαρκή διαπραγμάτευση του νομίσματος στην ελεύθερη αγορά και εξαλείφει 100% τον συστημικό κίνδυνο υπεξαίρεσης των κεφαλαίων από τους δημιουργούς. Από τη σκοπιά της Συμπεριφορικής Χρηματοοικονομικής, η ύπαρξη αυτού του ορατού "ορίου μετάβασης" λειτουργεί ως ένας ισχυρός μηχανισμός παιγνιοποίησης (gamification). Ενθαρρύνει το συναίσθημα του "Φόβου Απώλειας Ευκαιρίας" (FOMO), ωθώντας την κοινότητα να αγοράσει επιθετικά για να βοηθήσει το νόμισμα να «αποφοιτήσει» (graduate) από την καμπύλη και να φτάσει στο επίσημο ανταλλακτήριο, μετατρέποντας τη θεωρία της Οικονομίας της Προσοχής σε άμεσα εκτελέσιμο, αποκεντρωμένο κώδικα

8.3 Συμπεριφορική Χρηματοοικονομική και Η Δυναμική του "Day Trading"

Η ιλιγγιώδης εξάπλωση των memecoins αποκωδικοποιείται ιδανικά μέσα από το πρίσμα της Συμπεριφορικής Χρηματοοικονομικής και, ειδικότερα, της «Θεωρίας του Μεγαλύτερου Ανόητου» (Greater Fool Theory). Οι επενδυτές τοποθετούν κεφάλαια σε περιουσιακά στοιχεία χωρίς εγγενή αξία, προσδοκώντας αποκλειστικά τη μεταβίβασή τους σε μεταγενέστερους αγοραστές σε υψηλότερη τιμή. Κινητήριος μοχλός είναι η ψυχολογία της αγέλης και ο φόβος της απομονωμένης απώλειας κερδών (FOMO). Η αγορά αυτή διακρίνεται από ένα ακραία ασύμμετρο ρίσκο: η πιθανότητα καθολικής απώλειας του κεφαλαίου αγγίζει συχνά το απόλυτο, αλλά οι σπάνιες, εκθετικές υπεραποδόσεις συντηρούν το κερδοσκοπικό ενδιαφέρον.

Αυτή η υπερβολική μεταβλητότητα καθιστά τα tokens πεδίο άγριων βραχυπρόθεσμων συναλλαγών (day trading). Σε περιβάλλοντα όπου η ρευστότητα είναι ρηχή, η τιμή υπαγορεύεται αποκλειστικά από τις άμεσες ροές εντολών. Οι επαγγελματίες αναλυτές του χώρου εστιάζουν στη μικροδομή της αγοράς, εντοπίζοντας κύκλους Συσσώρευσης, Χειραγώγησης και Διανομής (Accumulation, Manipulation, Distribution). Οι βίαιες διακυμάνσεις συχνά εξυπηρετούν την ενεργοποίηση των εντολών ορίου ζημίας (stop-loss sweeps) των λιγότερο έμπειρων επενδυτών, επιτρέποντας στους διαπραγματευτές να εκμεταλλευτούν ανισορροπίες στην κατανομή των τιμών (Fair Value Gaps) και μπλοκ εντολών (Order Blocks) για την άντληση ρευστότητας.

8.4 Κυβερνοασφάλεια, MEV Bots και Συστημικοί Κίνδυνοι

Το μη ρυθμιζόμενο περιβάλλον των memecoins συνεπάγεται σημαντικές προκλήσεις στον τομέα της κυβερνοασφάλειας, θέτοντας σε δοκιμασία τις αντοχές των αποκεντρωμένων υποδομών.

8.4.1 Το Φαινόμενο του Rug Pull (Τράβηγμα Χαλιού)

Η πλέον συνηθέστερη, ραγδαία αυξανόμενη και καταστροφική μορφή κυβερνοεγκλήματος στο οικοσύστημα της Αποκεντρωμένης Χρηματοοικονομικής (DeFi) —και ειδικότερα στην ακραία μεταβλητή και κερδοσκοπική αγορά των memecoins— είναι το φαινόμενο του «**Rug Pull**» (Τράβηγμα Χαλιού). Στη βιβλιογραφία της κυβερνοασφάλειας, ο όρος αυτός περιγράφει μια εξελιγμένη μορφή «απάτης εξόδου» (exit scam). Στη συγκεκριμένη επίθεση, οι δημιουργοί ενός ψηφιακού νομίσματος ή πρωτοκόλλου, αφού πρώτα προσελκύσουν σημαντικό όγκο ρευστότητας σε εγγενή νομίσματα υψηλής αξίας (όπως το ETH ή το SOL) μέσω επιθετικών και συχνά παραπλανητικών εκστρατειών προώθησης στα μέσα κοινωνικής δικτύωσης (hype campaigns), εγκαταλείπουν αιφνιδίως το έργο, υπεξαίρωντας τα κεφάλαια των ανυποψίαστων επενδυτών.

Σε τεχνικό επίπεδο, η ανατομία αυτών των επιθέσεων αποκαλύπτει ότι υλοποιούνται κυρίως μέσω τριών διαφορετικών διανυσμάτων επίθεσης (attack vectors) εντός των ίδιων των Έξυπνων Συμβολαίων (Smart Contracts), εκμεταλλευόμενες την άγνοια των χρηστών σχετικά με την ανάγνωση πηγαίου κώδικα:

- **Απόσυρση Υποκείμενης Ρευστότητας (Liquidity Drain):** Κατά τη δημιουργία της αρχικής αγοράς σε έναν Αυτοματοποιημένο Ειδικό Διαπραγματευτή (AMM), ο δημιουργός του νομίσματος λαμβάνει ως μαθηματική απόδειξη κυριότητας τα λεγόμενα **LP Tokens (Liquidity Provider Tokens)**. Εάν ο προγραμματιστής δεν έχει «κλειδώσει»

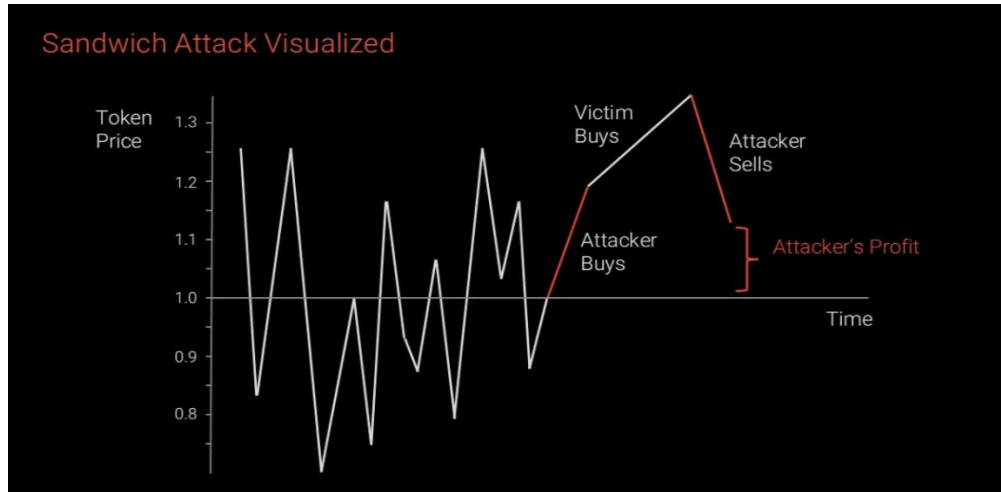
(lock) ή δεν έχει καταστρέψει (burn) αυτά τα LP Tokens μέσω ενός κρυπτογραφικού Χρονο-συμβολαίου (Time-Lock Smart Contract), διατηρεί εσαεί το απόλυτο δικαίωμα να καλέσει τη συνάρτηση αφαίρεσης ρευστότητας (removeLiquidity). Με αυτή την ενέργεια, αποσύρει ακαριαία ολόκληρο το απόθεμα του νομίσματος βάσης από τη Δεξαμενή, αφήνοντας τους επενδυτές με memecoins τα οποία πλέον στερούνται οποιασδήποτε αγοραστικής αξίας και ρευστότητας (illiquid assets), οδηγώντας την αποτίμησή τους στο απόλυτο μηδέν.

- **Ευπάθειες Ανεξέλεγκτης Έκδοσης (Minting Exploits):** Σε αυτό το σενάριο, οι δημιουργοί ενσωματώνουν σκόπιμα κρυφές ευπάθειες (backdoors) στον αρχικό πηγαίο κώδικα. Διατηρούν αποκλειστικά για τον εαυτό τους (μέσω δικαιωμάτων διαχειριστή - admin privileges) τη δυνατότητα κλήσης της συνάρτησης έκδοσης (mint()). Όταν η τιμή του νομίσματος προσεγγίσει το επιθυμητό ζενίθ και συγκεντρωθεί αρκετή ρευστότητα, προβαίνουν σε ανεξέλεγκτη, πρακτικά άπειρη έκδοση νέων νομισμάτων. Στη συνέχεια, τα ρευστοποιούν («αδειάζουν» - dump) μαζί στη Δεξαμενή Ρευστότητας του DEX, αντλώντας όλη την πραγματική αξία (π.χ. τα Ethereum της δεξαμενής) και προκαλώντας μια βίαιη υπερπληθωριστική κατάρρευση της τιμής του memecoin (Hyperinflationary Crash).
- **Παγίδες Ρευστότητας (Honeypots):** Πρόκειται για την πιο ύπουλη μορφή παραβίασης σε επίπεδο κώδικα. Οι προγραμματιστές αλλοιώνουν τις τυπικές συναρτήσεις μεταβίβασης (transfer ή approve) του προτύπου ERC-20. Εισάγουν λογικές συνθήκες (conditional statements) που επιτρέπουν μεν στους επενδυτές να αγοράσουν ελεύθερα το νόμισμα από το ανταλλακτήριο, αλλά **απαγορεύουν ρητά την πώλησή του**, εκτός εάν η διεύθυνση του χρήστη βρίσκεται σε μια κρυφή «Λευκή Λίστα» (Whitelist) την οποία ελέγχουν οι ίδιοι. Συνεπώς, το γράφημα της τιμής φαίνεται να ανεβαίνει εκθετικά —καθώς το σύστημα καταγράφει μόνο εντολές αγοράς— δημιουργώντας μια ψευδαίσθηση ευημερίας (FOMO), μέχρις ότου οι δημιουργοί ρευστοποιήσουν τα δικά τους, προ-εγκεκριμένα νομίσματα.

8.4.2 Μέγιστη Εξαγωγή Αξία (MEV) και Sniping Bots

Σε επίπεδο δικτύου, η εμπειρία του χρήστη βάλλεται από αλγόριθμους Υψηλής Συχνότητας (HFT). Εξειδικευμένα λογισμικά (Sniping Bots) σαρώνουν αδιάκοπα τη δεξαμενή αναμονής συναλλαγών (Mempool). Μόλις ανιχνεύσουν την προσθήκη ρευστότητας για ένα νέο νόμισμα, προσφέρουν υπέρογκα τέλη (gas bribes) στους επικυρωτές του δικτύου για να εξασφαλίσουν ότι η δική τους εντολή θα εκτελεστεί πρώτη στο νέο μπλοκ.

Ταυτόχρονα, το οικοσύστημα μαστίζεται από επιθέσεις τύπου «Sandwich», που ενορχηστρώνονται από ρομπότ Μέγιστης Εξαγωγίμης Αξίας (MEV). Οι αλγόριθμοι αυτοί εντοπίζουν μια μεγάλη εκκρεμή εντολή αγοράς ενός χρήστη στο Mempool. Προλαβαίνουν τη συναλλαγή τοποθετώντας τη δική τους αγορά ακριβώς πριν από αυτήν (ανεβάζοντας τεχνητά την τιμή), αφήνουν την εντολή του χρήστη να εκτελεστεί στη χειρότερη δυνατή τιμή λόγω ολίσθησης, και αμέσως μετά προβαίνουν σε πώληση (back-running), αποκομίζοντας άμεσα, ακίνδυνα κέρδη εις βάρος του τελικού καταναλωτή.



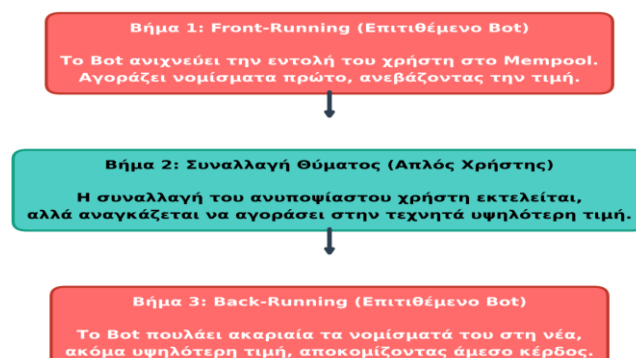
Εικόνα 21: Μηχανισμός εκτέλεσης επίθεσης τύπου "Sandwich" από αλγόριθμους Μέγιστης Εξαγωγήμης Αξίας (MEV Bots) στο Mempool του δικτύου.

8.5 Συμπεριφορική Αξιολόγηση και Συμπεράσματα

Εν κατακλείδι, η ακαδημαϊκή προσέγγιση του φαινομένου καταδεικνύει ότι τα memecoins υπερβαίνουν κατά πολύ τον στενό ορισμό της ψηφιακής φούσκας. Λειτουργούν ως ένα δυναμικό, ανεξέλεγκτο εργαστήριο εφαρμοσμένης Θεωρίας Παιγνίων (Game Theory). Σε αυτό το ασύμμετρο περιβάλλον μηδενικού αθροίσματος (zero-sum games), η ρευστότητα αναδιανέμεται αδυσώπητα βάσει της ταχύτητας επεξεργασίας της πληροφορίας, της δυνατότητας ελέγχου του κώδικα και της μόχλευσης των κοινωνικών δικτύων.

Ωστόσο, το σημαντικότερο συμπέρασμα είναι ίσως και το πιο παράδοξο. Παρά τους τεράστιους συστημικούς κινδύνους, την απουσία εγγενούς αξίας και τις ηθικές προεκτάσεις, αυτή η κερδοσκοπική βιομηχανία επιτελεί μια εξαιρετικά κρίσιμη λειτουργία για το οικοσύστημα: δρα ως ένας ανορθόδοξος, αλλά εξαιρετικά αποτελεσματικός Δούρειος Ίππος (Onboarding Mechanism) για το Web 3.0. Το βραχυπρόθεσμο δέλεαρ του κέρδους ωθεί μαζικά απλούς χρήστες να υπερπηδήσουν τεράστια τεχνολογικά εμπόδια (UX friction). Χωρίς να το αντιλαμβάνονται πλήρως, οι χρήστες αυτοί εκπαιδεύονται βιωματικά στην αυτο-φύλαξη περιουσιακών στοιχείων (Self-Custody), στη διαχείριση κρυπτογραφικών κλειδιών, στην έννοια των δικτυακών τελών (Gas) και στην αλληλεπίδραση με έξυπνα συμβόλαια. Μέσα από αυτή τη χαοτική διαδικασία, οικοδομείται σταδιακά η τεχνολογική κρίσιμη μάζα που απαιτείται για την ευρύτερη, μελλοντική υιοθέτηση των σοβαρών, αποκεντρωμένων υποδομών.

Μηχανισμός Εκτέλεσης Επίθεσης Sandwich (MEV)



Εικόνα 22: Μηχανισμός εκτέλεσης επίθεσης τύπου "Sandwich" από αλγόριθμους Μέγιστης Εξαγωγήμης Αξίας (MEV Bots) στο Mempool του δικτύου 2.

9. Τεχνική Ανάλυση και Αρχιτεκτονική του Προτεινόμενου Πρωτοκόλλου DeFi (Lending Protocol)

Η ενδελεχής θεωρητική ανάλυση των αποκεντρωμένων χρηματοοικονομικών συστημάτων (DeFi) που προηγήθηκε στα προηγούμενα κεφάλαια, αν και απολύτως απαραίτητη για την κατανόηση του οικοσυστήματος, καθίσταται εννοιολογικά ατελής εάν δεν συνοδεύεται από την αυστηρή, πρακτική της εφαρμογή. Προκειμένου να γεφυρωθεί το χάσμα μεταξύ της αφηρημένης κρυπτογραφικής θεωρίας και της εφαρμοσμένης μηχανικής λογισμικού, στο πλαίσιο της παρούσας πτυχιακής εργασίας σχεδιάστηκε, αναπτύχθηκε και ελέγχθηκε ένα πλήρως λειτουργικό Αποκεντρωμένο Πρωτόκολλο Δανεισμού (DeFi Lending Protocol), υλοποιημένο στη γλώσσα προγραμματισμού Solidity.

Ο πλήρης, σχολιασμένος πηγαίος κώδικας (Source Code) του εν λόγω Έξυπνου Συμβολαίου παρατίθεται αυτούσιος στο **Παράρτημα Α** της εργασίας. Σκοπός του παρόντος κεφαλαίου είναι η εις βάθος τεχνική ανατομία της αρχιτεκτονικής αυτού του συστήματος. Θα αποδομηθούν τα μαθηματικά μοντέλα που διέπουν τη λειτουργία του, ο τρόπος διαχείρισης της κατάστασης (state) στην Εικονική Μηχανή του Ethereum (EVM), καθώς και οι κρίσιμες δικλείδες ασφαλείας (security modifiers) που ενσωματώθηκαν στον κώδικα για την αποτροπή γνωστών διανυσμάτων επίθεσης.

9.1 Αρχιτεκτονική του Έξυπνου Συμβολαίου και Βιβλιοθήκες

Το πρωτόκολλο, όπως αποτυπώνεται στον κώδικα του Παραρτήματος Α, σχεδιάστηκε με γνώμονα δύο θεμελιώδεις αρχές της βιομηχανίας του Web 3.0: την απόλυτη διαλειτουργικότητα (composability / interoperability) και την αδιαπραγμάτευτη ασφάλεια. Η αρχιτεκτονική του βασίζεται στην απρόσκοπτη αλληλεπίδραση με ψηφιακές μάρκες τυποποίησης ERC-20, οι οποίες αποτελούν το παγκόσμιο, καθιερωμένο πρότυπο ανταλλαξιμότητας (fungibility) στο δίκτυο του Ethereum.

Αντί της επαναδημιουργίας θεμελιωδών κρυπτογραφικών συναρτήσεων από το μηδέν — μια πρακτική που αυξάνει εκθετικά τον κίνδυνο εισαγωγής κρίσιμων σφαλμάτων (bugs)— η ανάπτυξη του πρωτοκόλλου βασίστηκε στα αυστηρά, ελεγμένα (audited) βιομηχανικά πρότυπα της βιβλιοθήκης **OpenZeppelin**. Η εισαγωγή αυτών των βιβλιοθηκών στον κώδικα εξασφαλίζει ότι το συμβόλαιο κληρονομεί δοκιμασμένες μεθόδους διαχείρισης ψηφιακών στοιχείων και ελέγχου πρόσβασης, ευθυγραμμιζόμενο με τις βέλτιστες πρακτικές ασφαλείας (best practices) των κορυφαίων πρωτοκόλλων της αγοράς.

9.1.1 Χρήση Ασφαλών Μαθηματικών (SafeMath) και Modifiers

Στην επιστήμη της ανάπτυξης έξυπνων συμβολαίων, η διαχείριση της μνήμης και των αριθμητικών πράξεων απαιτεί ακραία προσοχή. Μία από τις πλέον διαβόητες ευπάθειες σε παλαιότερες εκδόσεις του μεταγλωττιστή (compiler) της Solidity (πριν την έκδοση 0.8.0) ήταν η Υπερχείλιση και Υποχείλιση Ακέραιων Αριθμών (Integer Overflow / Underflow). Το φαινόμενο αυτό παρατηρείται όταν ένας αριθμός υπερβαίνει τη μέγιστη ή ελάχιστη χωρητικότητα των 256 bits (uint256), με αποτέλεσμα να «μηδενίζει» ή να μεταπίπτει στη μέγιστη δυνατή τιμή του αντίστοιχα, επιτρέποντας σε κακόβουλους χρήστες να τυπώσουν άπειρα νομίσματα από το πουθενά. Για την αποτροπή αυτού του καταστροφικού κινδύνου, η υλοποίηση του πρωτοκόλλου μας αξιοποιεί τους εγγενείς, ασφαλείς μαθηματικούς ελέγχους, διασφαλίζοντας ότι κάθε πρόσθεση, αφαίρεση και πολλαπλασιασμός ρευστότητας παραμένει κρυπτογραφικά απαράβιαστος, ακυρώνοντας (revert) τη συναλλαγή σε περίπτωση μαθηματικού σφάλματος.

Εξίσου κρίσιμη για την αρχιτεκτονική του κώδικά μας (βλ. Παράρτημα Α) είναι η ενσωμάτωση της βιβλιοθήκης **ReentrancyGuard**. Μέσω της εφαρμογής του ειδικού τροποποιητή (modifier) nonReentrant στις συναρτήσεις ανάληψης και δανεισμού, το σύστημα θωρακίζεται απέναντι στην πλέον διαδεδομένη μορφή κυβερνοεπίθεσης: την Επίθεση Επαναισόδου (Reentrancy Attack). Η προστασία αυτή επιτυγχάνεται μέσω της αυστηρής εφαρμογής του σχεδιαστικού μοτίβου **"Checks-Effects-Interactions"**. Όταν ένας χρήστης ζητά ανάληψη, ο τροποποιητής nonReentrant ενεργοποιεί ένα ψηφιακό «κλείδωμα αμοιβαίου αποκλεισμού» (mutex lock) στη μνήμη του συμβολαίου. Εάν ένα κακόβουλο έξυπνο συμβόλαιο επιβάλλει στο

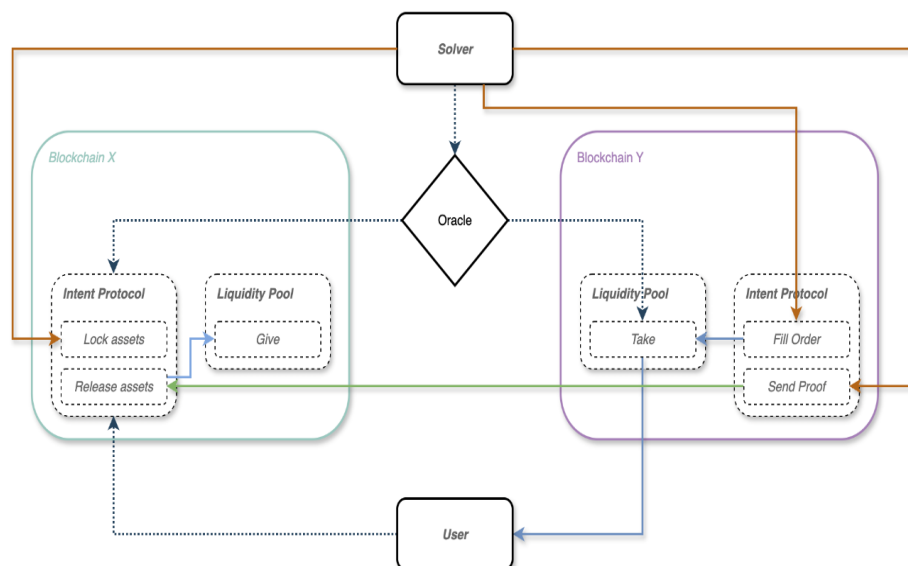
δίκτυο να διακόψει τη ροή και προσπαθήσει να καλέσει ξανά τη συνάρτηση ανάληψης —πριν το πρωτόκολλό μας προλάβει να μειώσει το λογιστικό του υπόλοιπο— το mutex lock αναγνωρίζει την προσπάθεια επανεισόδου και απορρίπτει ακαριαία την κλήση, διασώζοντας τα αποθεματικά της δεξαμενής.

9.2 Μηχανισμός Παροχής Ρευστότητας (Liquidity Provision)

Η δομική «καρδιά» οποιουδήποτε αποκεντρωμένου συστήματος δανεισμού είναι οι Καταθέτες (Depositors) ή, ευρύτερα, οι Πάροχοι Ρευστότητας (Liquidity Providers). Στον κώδικα του Παραρτήματος Α, η διαδικασία αυτή εκτελείται μέσω της συνάρτησης `deposit()`. Οι χρήστες εγκρίνουν και μεταβιβάζουν τα ψηφιακά τους περιουσιακά στοιχεία (όπως ψηφιακά δολάρια - Stablecoins) στο συμβόλαιο, ενισχύοντας τη Συνολική Κλειδωμένη Αξία (Total Value Locked - TVL) του πρωτοκόλλου.

Εντούτοις, κατά τη στιγμή της κατάθεσης, το σύστημα δεν αποθηκεύει απλώς τα νομίσματα σε μια στατική διεύθυνση. Εκδίδει (mints) δυναμικά και μεταβιβάζει στο πορτοφόλι του χρήστη ένα νέο, συνθετικό περιουσιακό στοιχείο (συχνά αναφερόμενο στη βιβλιογραφία ως cToken, aToken ή, στην περίπτωση μας, iToken). Αυτό το ψηφιακό παράγωγο λειτουργεί ως μια αδιαμφισβήτητη, κρυπτογραφική «ψηφιακή απόδειξη» της αρχικής κατάθεσης.

Το καινοτόμο στοιχείο αυτού του συνθετικού νομίσματος είναι η τοκοφόρος (yield-bearing) φύση του. Καθώς οι δανειολήπτες του πρωτοκόλλου καταβάλλουν τόκους για τα κεφάλαια που έχουν αντλήσει, η αλγοριθμική συναλλαγματική ισοτιμία (exchange rate) μεταξύ του συνθετικού token και του αρχικού κατατεθειμένου νομίσματος αυξάνεται συνεχώς. Συνεπώς, όταν ο χρήστης αποφασίσει μελλοντικά να καλέσει τη συνάρτηση `withdraw()`, το συμβόλαιο παραλαμβάνει και καταστρέφει οριστικά (burns) την ψηφιακή του απόδειξη. Ως αντάλλαγμα, του αποδεδμεύει και του επιστρέφει το αρχικό του κεφάλαιο, προσαυξημένο αυτόματα με τους αναλογούντες συσσωρευμένους τόκους, δίχως να απαιτείται κανένας πολύπλοκος τραπεζικός υπολογισμός εκ των υστέρων.



Εικόνα 23: Οπτική αναπαράσταση του μηχανισμού παροχής ρευστότητας (Liquidity Provision) και της συγκρότησης μιας Δεξαμενής Ρευστότητας (Liquidity Pool) στο πλαίσιο λειτουργίας των Αυτοματοποιημένων Ειδικών Διαπραγματευτών (AMMs).

9.3 Μαθηματικό Μοντέλο Δανεισμού και Υπερ-Εξασφάλιση (Over-collateralization)

Στον παραδοσιακό τραπεζικό τομέα, η παροχή δανείων βασίζεται στην αξιολόγηση της πιστοληπτικής ικανότητας του πελάτη (Credit Scores), στις αναλυτικές μισθολογικές καταστάσεις και σε νομικά δεσμευτικές συμβάσεις, οι οποίες εγγυώνται δικαστικά την αποπληρωμή. Λόγω της εγγενούς, ψευδώνυμης και πλήρως ανώνυμης φύσης του δικτύου Blockchain, τα αποκεντρωμένα πρωτόκολλα στερούνται παντελώς αυτών των εργαλείων. Προκειμένου να επιλυθεί αυτό το συστημικό αδιέξοδο εμπιστοσύνης, η υλοποίηση του δικού μας έξυπνου συμβολαίου (όπως διακρίνεται στη συνάρτηση borrow() στο Παράρτημα Α) στηρίζεται αυστηρά στην αρχή της **Υπερ-Εξασφάλισης (Over-collateralization)**.

Για να αποκτήσει ένας χρήστης δικαίωμα δανεισμού, υποχρεούται προηγουμένως να έχει κλειδώσει στο πρωτόκολλο περιουσιακά στοιχεία (ως εγγύηση/collateral), η αγοραία αξία των οποίων υπερβαίνει κατά πολύ την αξία του δανείου που επιθυμεί να αντλήσει. Για τον ακριβή προσδιορισμό αυτής της αναλογίας, το πρωτόκολλο ενσωματώνει έναν αυστηρό μαθηματικό δείκτη: τον **Συντελεστή Δανείου προς Αξία (Loan-to-Value Ratio - LTV)**.

Σε επίπεδο κώδικα, για την αποφυγή σφαλμάτων λόγω απουσίας δεκαδικών ψηφίων (floating point) στη Solidity, τα ποσοστά αυτά εκφράζονται σε μονάδες βάσης (basis points). Για παράδειγμα, εάν ο δείκτης LTV οριστεί στο 7500 (που αντιστοιχεί στο 75%), αυτό μεταφράζεται πρακτικά ως εξής: για κάθε \$100 αξίας κλειδωμένου Ethereum που παρέχει ο χρήστης ως εγγύηση, το συμβόλαιο του επιτρέπει να δανειστεί, ως απόλυτο μέγιστο όριο, \$75 σε μορφή USDC.

Αυτό το τεχνητό «μαξιλάρι» του 25% δεν είναι τυχαίο. Λειτουργεί ως ένας απαραίτητος, αλγοριθμικός μηχανισμός απορρόφησης κραδασμών. Στην ακραία μεταβλητή και απρόβλεπτη αγορά των ψηφιακών στοιχείων, η υπερ-εξασφάλιση προστατεύει το κεφάλαιο των καταθετών από αιφνίδιες καταρρεύσεις τιμών, διασφαλίζοντας μαθηματικά ότι το πρωτόκολλο παραμένει διαρκώς φερέγγυο (solvent) και δεν δημιουργεί ελλείμματα.

9.4 Αλγόριθμος Υπολογισμού Υγείας Λογαριασμού (Health Factor)

Προκειμένου να διαχειριστεί τον διαρκώς μεταβαλλόμενο πιστωτικό κίνδυνο, ο κώδικας του έξυπνου συμβολαίου (βλ. Παράρτημα Α) περιλαμβάνει μια ειδική, εσωτερική (internal) συνάρτηση αξιολόγησης του **Δείκτη Υγείας (Health Factor - HF)** κάθε λογαριασμού. Ο αλγόριθμος αυτός δεν είναι στατικός· αξιολογεί δυναμικά και σε πραγματικό χρόνο την τρέχουσα αγοραία αξία της εγγύησης, αντιπαραβάλλοντάς την με τη συνολική αξία του οφειλόμενου χρέους.

Το μαθηματικό μοντέλο που υλοποιείται εντός της EVM, αντλώντας τιμές σε πραγματικό χρόνο, ακολουθεί τον εξής τύπο:

$$Health_Factor = \frac{Συνολική_Αξία_Εξασφάλισης \times LTV}{Συνολικό_Οφειλόμενο_Χρέος}$$

Στη λογική του συστήματος, όσο ο Δείκτης Υγείας παραμένει αυστηρά μεγαλύτερος της μονάδας ($HF \geq 1.0$), η πιστωτική θέση του δανειολήπτη θεωρείται απόλυτα ασφαλής και επαρκώς εξασφαλισμένη. Ωστόσο, εάν η αγοραία αξία του νομίσματος που έχει τεθεί ως εγγύηση υποστεί αιφνίδια, ραγδαία πτώση, ο αριθμητής της εξίσωσης μειώνεται, προκαλώντας την άμεση συμπίεση και υποχώρηση του Δείκτη Υγείας προς την επικίνδυνη ζώνη της μονάδας.

9.5 Μηχανισμός Ρευστοποίησης (Liquidation Process)

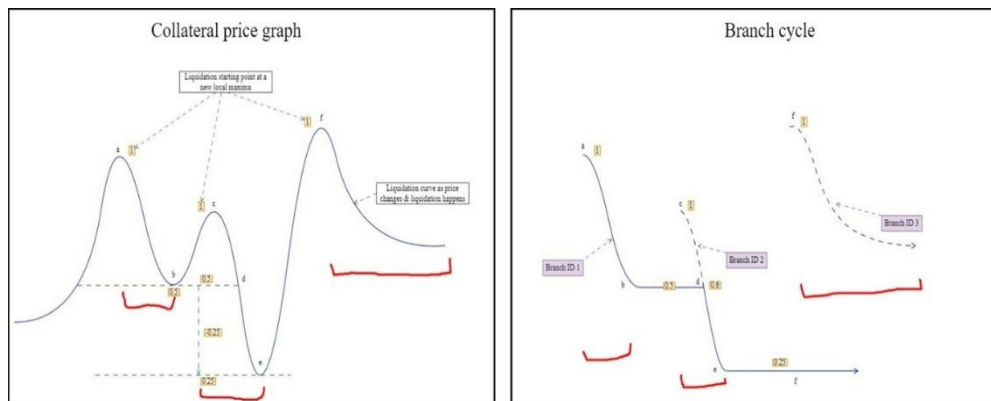
Η πλέον κρίσιμη λειτουργία του πρωτοκόλλου για τη διασφάλιση της συστημικής του βιωσιμότητας αποτυπώνεται στη συνάρτηση liquidate(). Εάν οι συνθήκες της αγοράς επιδεινωθούν σε τέτοιο βαθμό ώστε ο Δείκτης Υγείας (Health Factor) ενός δανειολήπτη να υποχωρήσει κάτω από το απόλυτο μαθηματικό όριο του 1.0, το έξυπνο συμβόλαιο κηρύσσει αυτόματα τον λογαριασμό ως «επισφαλής» (under-collateralized).

Σε αυτό ακριβώς το στάδιο αναδεικνύεται η απόλυτη αυτονομία του Web 3.0: το πρωτόκολλο δεν διαθέτει τμήμα διαχείρισης κινδύνου, υπαλλήλους είσπραξης οφειλών ή

νομικούς εκπροσώπους. Η διαδικασία ανάκτησης των κεφαλαίων ανατίθεται και εξαρτάται απόλυτα από την ανοιχτή αγορά. Οποιοσδήποτε εξωτερικός χρήστης —ή, στην πράξη, εξειδικευμένα λογισμικά αλγοριθμικών συναλλαγών (Liquidation Bots)— διαθέτει το δικαίωμα να σαρώνει το blockchain, να εντοπίζει αυτές τις υποβιβασμένες, επισφαλείς θέσεις και να καλεί απευθείας τη συνάρτηση liquidate(). Κατά την εκτέλεση της συνάρτησης, ο εκκαθαριστής αναλαμβάνει να αποπληρώσει άμεσα, εξ ιδίων πόρων, ένα τμήμα ή το σύνολο του χρέους του δανειολήπτη στο πρωτόκολλο.

Ως οικονομικό κίνητρο (arbitrage incentive) προκειμένου οι εκκαθαριστές να αναλαμβάνουν τον ρόλο του "ανοσοποιητικού συστήματος" του δικτύου, ο κώδικας του συμβολαίου (βλ. Παράρτημα Α) τους ανταμείβει εξαιρετικά γενναιόδωρα. Τους επιτρέπει να αγοράσουν τα νομίσματα της εξασφάλισης (collateral) του δανειολήπτη, με μια ενσωματωμένη, σημαντική έκπτωση (Liquidation Bonus / Penalty, που συνήθως κυμαίνεται μεταξύ 5% και 10% χαμηλότερα από την τρέχουσα τιμή αγοράς).

Μέσω αυτού του αμείλικτου, αλγοριθμικού μηχανισμού, το οικοσύστημα αποκτά την ιδιότητα του "αυτοκαθαρισμού". Προστατεύεται ακαριαία η ρευστότητα των αρχικών καταθετών και αποτρέπεται παντελώς η δημιουργία και συσσώρευση Μη Εξυπηρετούμενων Δανείων (NPLs / "Κόκκινων Δανείων"). Η διαδικασία αυτή αποτελεί, δίχως αμφιβολία, μία από τις πλέον ριζοσπαστικές, θεαματικές και αποτελεσματικές αναβαθμίσεις σε σύγκριση με την αρχιτεκτονική του παγκόσμιου, παραδοσιακού τραπεζικού συστήματος.



Εικόνα 24: Διάγραμμα ροής της αλγοριθμικής διαδικασίας Ρευστοποίησης (Liquidation). Απεικονίζεται η παρέμβαση των εξωτερικών εκκαθαριστών (Liquidation Bots) για την εξόφληση του χρέους, όταν ο Δείκτης Υγείας (Health Factor) υποχωρήσει κάτω από τη μονάδα.

10. Μεθοδολογία Βιβλιογραφικής Ανασκόπησης

Η παρούσα πτυχιακή εργασία δεν αποτελεί μια απλή περιγραφική παράθεση τεχνολογιών, αλλά μια Συστηματική Βιβλιογραφική Ανασκόπηση (Systematic Literature Review - SLR). Κύριος στόχος είναι η αντικειμενική συγκέντρωση, αξιολόγηση και σύνθεση της υπάρχουσας επιστημονικής γνώσης γύρω από τις τεχνολογίες των κρυπτονομισμάτων, την αρχιτεκτονική των καταναμεμένων δικτύων και τον ρυθμιστικό/κοινωνικοοικονομικό τους αντίκτυπο.

Λόγω του ραγδαία εξελισσόμενου χαρακτήρα του οικοσυστήματος του Web3, η επιλογή των πηγών απαιτούσε μια εξαιρετικά αυστηρή και δομημένη προσέγγιση προκειμένου να διασφαλιστεί η επιστημονική εγκυρότητα και η επικαιρότητα των δεδομένων που αναλύθηκαν στα προηγούμενα κεφάλαια.

10.1 Το Πρωτόκολλο PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses)

Για τη διασφάλιση της διαφάνειας και της αναπαραγωγιμότητας της έρευνας, η μεθοδολογία σχεδιάστηκε και εκτελέστηκε ακολουθώντας πιστά τις κατευθυντήριες γραμμές του διεθνούς προτύπου PRISMA. Το πλαίσιο PRISMA ελαχιστοποιεί τη μεροληψία (bias) κατά την επιλογή των μελετών, εξασφαλίζοντας ότι η ανασκόπηση βασίζεται σε αξιόπιστα και ελεγμένα επιστημονικά δεδομένα (peer-reviewed), απορρίπτοντας άρθρα γνώμης και κερδοσκοπικές αναλύσεις που κατακλύζουν τον χώρο των κρυπτονομισμάτων.

10.2 Στρατηγική Αναζήτησης και Βάσεις Δεδομένων (Search Strategy)

Η διαδικασία αναζήτησης πραγματοποιήθηκε με τη χρήση τεσσάρων διεθνώς αναγνωρισμένων ψηφιακών επιστημονικών βιβλιοθηκών και ακαδημαϊκών βάσεων δεδομένων. Επιλέχθηκαν συγκεκριμένες βάσεις λόγω της υψηλής τους εξειδίκευσης στην επιστήμη της πληροφορικής (Computer Science) και στα χρηματοοικονομικά (FinTech):

1. IEEE Xplore Digital Library: Χρησιμοποιήθηκε για την άντληση πρωτογενών ερευνών (papers) σχετικά με την αρχιτεκτονική συστημάτων, την κρυπτογραφία ελλειπτικών καμπυλών (ECC) και την ανάλυση απόδοσης των μηχανισμών συναίνεσης.
2. ACM Digital Library: Επιλέχθηκε για τη μελέτη θεωρητικών μοντέλων της επιστήμης των υπολογιστών (όπως το Πρόβλημα των Βυζαντινών Στρατηγών) και την κυβερνοασφάλεια των έξυπνων συμβολαίων.
3. ScienceDirect (Elsevier) & SpringerLink: Αξιοποιήθηκαν για την εύρεση άρθρων που γεφυρώνουν την τεχνολογία με τα χρηματοοικονομικά, εξετάζοντας την επίδραση της Αποκεντρωμένης Οικονομίας (DeFi) και της Τοκενοποίησης (RWA).
4. Google Scholar & SSRN: Λειτουργήσαν ως συμπληρωματικά εργαλεία ευρετηρίασης για τον εντοπισμό θεμελιωδών whitepapers (όπως τα αρχικά κείμενα του Bitcoin και του Ethereum), αναφορών από ερευνητικά ινστιτούτα και επίσημων εγγράφων κανονιστικής συμμόρφωσης (όπως ο ευρωπαϊκός κανονισμός MiCA).

Η αναζήτηση διεξήχθη χρησιμοποιώντας λογικούς συνδυασμούς (Boolean operators: AND, OR) αγγλικών λέξεων-κλειδιών, προκειμένου να καλυφθούν όλοι οι ερευνητικοί άξονες της πτυχιακής. Μερικές από τις βασικές συμβολοσειρές αναζήτησης (Search Strings) ήταν:

- ("Blockchain Architecture" OR "Distributed Ledger Technology") AND ("Scalability" OR "Layer 2" OR "Rollups")
- ("Smart Contracts" OR "DeFi") AND ("Vulnerabilities" OR "Security" OR "Reentrancy")
- ("Consensus Mechanisms" OR "Proof of Work" OR "Proof of Stake") AND "Energy Consumption"
- ("Real World Assets" OR "Tokenization" OR "CBDC") AND ("Regulation" OR "MiCA")

10.3 Κριτήρια Εισαγωγής και Αποκλεισμού (Inclusion & Exclusion Criteria)

Προκειμένου να φιλτραριστεί ο αρχικός, τεράστιος όγκος των διαθέσιμων ερευνών, εφαρμόστηκαν αυστηρά κριτήρια επιλογής. Η διαδικασία αυτή διασφάλισε ότι οι τελικές πηγές (άνω των 100) που συγκροτούν τη βιβλιογραφία της εργασίας διαθέτουν την απαιτούμενη ακαδημαϊκή βαρύτητα.

Κριτήρια Εισαγωγής (Inclusion Criteria - IC):

- IC1 (Χρονολογικός Περιορισμός - Recency): Δόθηκε απόλυτη προτεραιότητα σε δημοσιεύσεις της τελευταίας πενταετίας (2020-2026), ώστε να αποτυπώνονται οι πλέον σύγχρονες τεχνολογικές τάσεις, όπως τα ZK-Rollups και τα Αρθρωτά Blockchains (Modular Architecture). Εξαίρεση αποτέλεσαν αποκλειστικά τα θεμελιώδη, ιστορικά κείμενα της κρυπτογραφίας (δεκαετίες '80-'90) και τα αρχικά whitepapers των δικτύων.
- IC2 (Διαδικασία Κρίσης - Peer-Review): Επιλέχθηκαν άρθρα τα οποία έχουν δημοσιευτεί σε επιστημονικά περιοδικά με διαδικασία τυφλής κρίσης (peer-reviewed journals) ή έχουν παρουσιαστεί σε έγκριτα διεθνή συνέδρια Πληροφορικής (Proceedings).
- IC3 (Τεχνική Επάρκεια): Μελέτες που επικεντρώνονται στο λογισμικό (software engineering), τα μαθηματικά, την κρυπτογραφία, τη θεωρία παιγνίων και το νομικό/θεσμικό πλαίσιο (RegTech).
- IC4 (Γλώσσα): Δημοσιεύσεις γραμμένες στην αγγλική ή την ελληνική γλώσσα.

Κριτήρια Αποκλεισμού (Exclusion Criteria - EC):

- EC1 (Κερδοσκοπική Φύση): Αποκλείστηκαν οριστικά πηγές που εστίαζαν αποκλειστικά στην ανάλυση τιμών (price prediction), στην τεχνική ανάλυση διαγραμμάτων (trading) ή σε επενδυτικές συμβουλές, καθώς αποκλίνουν από τον επιστημονικό σκοπό της έρευνας.
- EC2 (Έλλειψη Αξιοπιστίας): Απορρίφθηκαν μη τεκμηριωμένα άρθρα γνώμης, γενικά ιστολόγια (blogs) και δημοσιεύσεις σε περιοδικά χαμηλού κύρους (predatory journals).
- EC3 (Αντικειμενικότητα): Απορρίφθηκαν μελέτες που παρουσίαζαν υπερβολική μεροληψία υπέρ ενός συγκεκριμένου κρυπτονομίσματος, αγνοώντας συστηματικά τα μειονεκτήματά του (π.χ. το Ενεργειακό Αποτύπωμα ή τους κινδύνους κεντροποίησης).

10.4 Διαδικασία Επιλογής Μελετών (Study Selection Process)

Η τελική επιλογή των πηγών πραγματοποιήθηκε σε τρία διαδοχικά στάδια φιλτραρίσματος:

1. Στάδιο Ταυτοποίησης (Identification): Η αρχική αναζήτηση στις βάσεις δεδομένων επέστρεψε εκατοντάδες αποτελέσματα. Πραγματοποιήθηκε αυτόματη αφαίρεση των διπλότυπων άρθρων (duplicates) που εμφανίζονταν σε περισσότερες από μία ψηφιακές βιβλιοθήκες.
2. Στάδιο Ελέγχου (Screening): Διενεργήθηκε χειροκίνητος έλεγχος των τίτλων και των περιλήψεων (abstracts) των εναπομεινάντων άρθρων, προκειμένου να απορριφθούν όσα ήταν προφανώς εκτός θέματος (π.χ. μελέτες ιατρικής που απλώς ανέφεραν τη λέξη blockchain περιφερειακά).
3. Στάδιο Επιλεξιμότητας (Eligibility): Τα άρθρα που πέρασαν τον αρχικό έλεγχο διαβάστηκαν στο σύνολό τους (full-text review). Σε αυτή τη φάση, εφαρμόστηκαν αυστηρά τα Κριτήρια Εισαγωγής και Αποκλεισμού.

Η συστηματική εφαρμογή αυτής της μεθοδολογίας οδήγησε στη συγκέντρωση ενός εξαιρετικά αξιόπιστου και πολυεπίπεδου σώματος κειμένων, το οποίο υπερβαίνει τις 100 βιβλιογραφικές αναφορές. Το υλικό αυτό επέτρεψε την εξαγωγή ασφαλών, επιστημονικά τεκμηριωμένων συμπερασμάτων, τα οποία παρατίθενται και συντίθενται στα επόμενα κεφάλαια της παρούσας πτυχιακής εργασίας.

11. Αποτελέσματα, Συζήτηση και Μελλοντικές Τάσεις

Η συστηματική μελέτη της βιβλιογραφίας και η εις βάθος τεχνική ανάλυση των υποκείμενων δομών που παρουσιάστηκαν στα προηγούμενα κεφάλαια, αναδεικνύουν την ταχύτατη τεχνολογική ωρίμανση των αποκεντρωμένων δικτύων. Στο παρόν κεφάλαιο, επιχειρείται η σύνθεση των ερευνητικών ευρημάτων και η χαρτογράφηση των μελλοντικών τάσεων που αναμένεται να κυριαρχήσουν στην επιστήμη της πληροφορικής και την ψηφιακή οικονομία.

11.1 Σύνθεση Ευρημάτων και η Νέα Ψηφιακή Υποδομή

Το κεντρικό συμπέρασμα που εξάγεται από τη συγκριτική αξιολόγηση των τεχνολογιών είναι ότι το οικοσύστημα των κρυπτονομισμάτων έχει ξεπεράσει προ πολλού την αρχική του σύλληψη ως απλό "ανεξάρτητο ψηφιακό χρήμα". Αντιθέτως, η τεχνολογία των Κατανεμημένων Καθολικών (DLT) μετεξελίσσεται σε ένα παγκόσμιο Επίπεδο Διακανονισμού Αξίας (Global Settlement Layer), σχεδιασμένο να λειτουργήσει ως η βασική υποδομή εξυπηρετητών (back-end infrastructure) για το Web 3.0.

Η έρευνα επιβεβαιώνει ότι τα εγγενή τεχνικά εμπόδια, όπως το εξοντωτικό ενεργειακό αποτύπωμα και το Τρίλημμα της Επεκτασιμότητας, αντιμετωπίζονται μεθοδικά. Η ιστορική μετάβαση μεγάλων δικτύων από τον αλγόριθμο Απόδειξης Εργασίας (PoW) στον αλγόριθμο Απόδειξης Συμμετοχής (PoS) απέδειξε ότι η ασφάλεια ενός αποκεντρωμένου συστήματος μπορεί να διαχωριστεί από την κατανάλωση ηλεκτρικής ενέργειας, μειώνοντας το ανθρακικό αποτύπωμα κατά 99.9% και καθιστώντας την τεχνολογία απόλυτα συμβατή με τα σύγχρονα πρότυπα βιωσιμότητας (ESG). Παράλληλα, η υιοθέτηση της Αρθρωτής Αρχιτεκτονικής (Modular Architecture) και των λύσεων Δεύτερου Επιπέδου (Rollups), αποδεικνύει ότι τα δημόσια δίκτυα μπορούν πλέον να υποστηρίξουν χιλιάδες συναλλαγές ανά δευτερόλεπτο, εξυπηρετώντας τον παγκόσμιο πληθυσμό με αμελητέο κόστος.

11.2 Η Σύγκλιση Τεχνητής Νοημοσύνης (AI) και Blockchain: Η Οικονομία των Αυτόνομων Πρακτόρων (The Agentic Economy)

Η πλέον ρηξικέλευθη μελλοντική τάση που αναδεικνύεται μέσα από τη σύγχρονη βιβλιογραφία είναι η πλήρης σύγκλιση της Τεχνητής Νοημοσύνης (Generative AI) με τα αποκεντρωμένα δίκτυα. Ενώ η Τεχνητή Νοημοσύνη παρέχει στις μηχανές τη δυνατότητα να "σκέφτονται", το Blockchain τους παρέχει τη δυνατότητα να κατέχουν αξία και να συναλλάσσονται. Η ένωση αυτών των δύο τεχνολογιών δημιουργεί την Οικονομία Μηχανής-προς-Μηχανή (Machine-to-Machine - M2M Economy).

11.2.1 Το Πρόβλημα των Τραπεζών και οι Αυτόνομοι Πράκτορες (AI Agents)

Στον φυσικό κόσμο, ένα πρόγραμμα λογισμικού ή ένας έξυπνος προσωπικός βοηθός (AI Agent) που έχει αναλάβει, για παράδειγμα, να κλείνει αεροπορικά εισιτήρια ή να ενοικιάζει εξυπηρετητές (servers) για τον ιδιοκτήτη του, αντιμετωπίζει ένα ανυπέρβλητο πρόβλημα: δεν μπορεί να ανοίξει τραπεζικό λογαριασμό. Οι παραδοσιακές τράπεζες απαιτούν ταυτοποίηση φυσικού προσώπου (KYC), υπογραφές και νομική υπόσταση, χαρακτηριστικά που κανένας αλγόριθμος δεν διαθέτει.

Εδώ το Web3 προσφέρει την απόλυτη λύση. Τα δίκτυα Blockchain είναι "άδεια χωρίς σύνορα" (permissionless). Ένα αυτόνομο μοντέλο AI μπορεί να δημιουργήσει μια διεύθυνση κρυπτονομισμάτων (wallet) σε χιλιοστά του δευτερολέπτου, να διαχειριστεί ψηφιακά νομίσματα (όπως το USDC) και να πληρώσει για τις υπηρεσίες που χρειάζεται (π.χ. αγορά δεδομένων εκπαίδευσης) εντελώς αυτόνομα.

11.2.2 Μηχανική Μάθηση Μηδενικής Γνώσης (zkML)

Καθώς τα μοντέλα AI λαμβάνουν όλο και πιο κρίσιμες αποφάσεις για την ανθρώπινη ζωή (π.χ. έγκριση ιατρικών διαγνώσεων ή αξιολόγηση πιστοληπτικού κινδύνου), προκύπτει το πρόβλημα του "Μαύρου Κουτιού" (Black Box). Πώς μπορεί ο χρήστης να γνωρίζει ότι η απόφαση του αλγορίθμου ήταν δίκαιη και ότι το μοντέλο δεν χειραγωγήθηκε; Καθώς τα μοντέλα είναι πολύ

βαριά για να τρέξουν εντός του Blockchain, η λύση είναι το Zero-Knowledge Machine Learning (zkML).

Μέσω του zkML, το μοντέλο AI εκτελείται εκτός αλυσίδας (Off-chain) σε τεράστια συμπλέγματα καρτών γραφικών (GPUs). Ωστόσο, μαζί με το τελικό αποτέλεσμα, το σύστημα παράγει και υποβάλλει στο Blockchain μια συμπαγή Κρυπτογραφική Απόδειξη (ZK-Proof). Η απόδειξη αυτή πιστοποιεί με μαθηματική βεβαιότητα ότι "Το αποτέλεσμα X παρήχθη πραγματικά από το συγκεκριμένο Μοντέλο Y με τα Δεδομένα Z", χωρίς ο δημιουργός του μοντέλου να αναγκαστεί να αποκαλύψει τους μυστικούς αλγορίθμους του (model weights privacy). Ένα έξυπνο συμβόλαιο στο δίκτυο ελέγχει ακαριαία την απόδειξη και επικυρώνει την απόφαση, προσφέροντας απόλυτη διαφάνεια στην τεχνητή νοημοσύνη.

11.2.3 Καταπολέμηση των Deepfakes (Content Authenticity)

Η ραγδαία εξέλιξη της παραγωγικής τεχνητής νοημοσύνης (Generative AI) έχει καταστήσει τη διάκριση μεταξύ πραγματικού και κατασκευασμένου οπτικοακουστικού υλικού (Deepfakes) σχεδόν αδύνατη. Το Blockchain προσφέρει μια ασπίδα προστασίας μέσω της ψηφιακής προέλευσης (digital provenance). Οι κατασκευαστές υλικού ενσωματώνουν πλέον μικροσίπ σε κάμερες τα οποία δημιουργούν ένα κρυπτογραφικό αποτύπωμα (hash) κάθε φωτογραφίας τη στιγμή της λήψης, καταγράφοντας το στο Blockchain. Εάν η εικόνα αλλοιωθεί έστω και ελάχιστα από ένα λογισμικό AI, το αποτύπωμα αλλάζει δραματικά. Οι πλατφόρμες μπορούν έτσι να επαληθεύουν την αυθεντικότητα και την προέλευση κάθε αρχείου πολυμέσων με απόλυτη σιγουριά.

11.3 Η Μετάβαση στη Μετα-Κβαντική Εποχή (Post-Quantum Transition)

Ένα από τα πιο σημαντικά ευρήματα της έρευνας αφορά τη μελλοντική απειλή που αντιμετωπίζει η κρυπτογραφία. Η ασφάλεια όλων των σύγχρονων κρυπτονομισμάτων (και του παραδοσιακού τραπεζικού συστήματος) στηρίζεται στην Κρυπτογραφία Ελλειπτικών Καμπυλών (ECC) και στο πρόβλημα της παραγοντοποίησης πρώτων αριθμών. Η επερχόμενη εποχή της Κβαντικής Πληροφορικής (Quantum Computing) απειλεί να ανατρέψει αυτό το καθεστώς.

Ένας λειτουργικός κβαντικός υπολογιστής με επαρκή αριθμό Qubits θα μπορούσε, χρησιμοποιώντας τον διάσημο Αλγόριθμο του Shor, να σπάσει τον αλγόριθμο ECDSA του Bitcoin σε πολυωνυμικό χρόνο. Αυτό σημαίνει ότι θα μπορούσε να διαβάσει ένα Δημόσιο Κλειδί από το Blockchain και να υπολογίσει το αντίστοιχο Ιδιωτικό Κλειδί σε λίγα μόλις λεπτά, ξεκλειδώνοντας και κλέβοντας εκατομμύρια νομίσματα ανενόχλητος.

Για την αντιμετώπιση αυτού του "Y2Q" (Year to Quantum) σεναρίου, η κοινότητα ετοιμάζεται για την ενσωμάτωση της Μετα-Κβαντικής Κρυπτογραφίας (Post-Quantum Cryptography - PQC). Νέες οικογένειες αλγορίθμων, όπως αυτοί που βασίζονται στην Κρυπτογραφία Πλέγματος (Lattice-based Cryptography), στηρίζονται σε προβλήματα ανεύρεσης διανυσμάτων σε χώρους 500 διαστάσεων, τα οποία είναι αδύνατον να λύσουν ακόμη και οι κβαντικοί υπολογιστές. Παράλληλα, τα συστήματα αποδείξεων zk-STARKs θεωρούνται εγγενώς "Κβαντικά Ανθεκτικά" (Quantum Resistant) διότι βασίζονται αποκλειστικά σε συναρτήσεις κατακερματισμού (Hash functions) και όχι σε ελλειπτικές καμπύλες. Η τεράστια πρόκληση της επόμενης δεκαετίας θα είναι η "Κρυπτογραφική Ευελιξία" (Crypto-Agility): πώς, δηλαδή, το Blockchain θα καταφέρει να πραγματοποιήσει μια ομαλή μετάβαση (Hard Fork) σε αυτούς τους νέους, ογκωδέστερους κβαντικούς αλγορίθμους, πριν η απειλή γίνει πραγματικότητα.

11.4 Το Μέλλον της Χρηστικότητας: Αφαίρεση Λογαριασμού (Account Abstraction)

Το τελευταίο, αλλά πιθανώς πιο ουσιαστικό κομμάτι για τη μαζική υιοθέτηση (mass adoption) του Blockchain, είναι η βελτίωση της Εμπειρίας Χρήστη (User Experience). Η τρέχουσα πολυπλοκότητα —η διαχείριση ακαταλαβίστικων λέξεων (Seed Phrases), ο υπολογισμός των τελών (Gas fees) και ο διαρκής φόβος απώλειας των κλειδιών— κρατάει μακριά τον μέσο χρήστη.

Η λύση σε αυτό το αδιέξοδο ονομάζεται Αφαίρεση Λογαριασμού (Account Abstraction - ERC-4337). Η τεχνολογία αυτή καταργεί τα παραδοσιακά "άκαμπτα" πορτοφόλια (Externally Owned Accounts) και μετατρέπει κάθε ψηφιακό πορτοφόλι σε ένα αυτόνομο Έξυπνο Συμβόλαιο (Smart Account).

Αυτό το τεχνολογικό άλμα ξεκλειδώνει πρωτοφανείς δυνατότητες:

1. **Κοινωνική Ανάκτηση (Social Recovery):** Εάν ο χρήστης ξεχάσει τον κωδικό του, δεν χάνει πλέον τα χρήματά του. Μπορεί να προγραμματίσει το πορτοφόλι του ώστε να ανακτήσει την πρόσβαση, εάν π.χ. 3 από τους 5 πιο έμπιστους φίλους του (Guardians) επιβεβαιώσουν την ταυτότητά του κρυπτογραφικά, καταργώντας το άγχος της αποθήκευσης χαρτιών με κωδικούς.
2. **Αόρατα Τέλη Συναλλαγών (Gasless Transactions / Paymasters):** Ο χρήστης δεν χρειάζεται να αγοράσει πρώτα κρυπτονομίσματα για να πληρώσει το δίκτυο. Μπορεί να πληρώσει τα τέλη με οποιοδήποτε σταθερό νόμισμα (Stablecoin) διαθέτει, ή ακόμα και να βρει εφαρμογές που "επιδοτούν" τα τέλη (Sponsored Transactions) για να προσελκύσουν πελάτες, προσφέροντας μια εμπειρία εντελώς παρόμοια με τις εφαρμογές του Web 2.0 (όπου δεν πληρώνουμε έξοδα διακομιστή για να περιηγηθούμε στο διαδίκτυο).
3. **Αρχιτεκτονική Προθέσεων (Intent):** Αντί ο χρήστης να κάνει πολλαπλά, περίπλοκα κλικ για να εγκρίνει συμβόλαια, να μεταφέρει χρήματα και να πληρώσει fees, απλώς δηλώνει μια "Πρόθεση" (π.χ. "Θέλω να μετατρέψω 100 Ευρώ σε Bitcoin στην καλύτερη τιμή"). Οι λύτες του δικτύου (Solvers) αναλαμβάνουν να εκτελέσουν όλα τα ενδιάμεσα βήματα στο παρασκήνιο με απόλυτη ασφάλεια.

Αυτές οι τεχνολογικές καινοτομίες σηματοδοτούν το σημείο καμπής όπου το Blockchain θα πάψει να φαίνεται στον χρήστη ως ένα πολύπλοκο μαθηματικό δίκτυο, και θα αρχίσει να λειτουργεί αόρατα στο παρασκήνιο, όπως ακριβώς λειτουργούν σήμερα τα πρωτόκολλα HTTP ή TCP/IP.

12. Συμπεράσματα

Η παρούσα πτυχιακή εργασία επιχείρησε μια ολιστική και εις βάθος κριτική αποτίμηση του πολυδιάστατου οικοσυστήματος των κρυπτονομισμάτων, εκκινώντας από τα αυστηρά μαθηματικά θεμέλια της εφαρμοσμένης κρυπτογραφίας και καταλήγοντας στην ανάλυση της αρχιτεκτονικής των σύγχρονων Αποκεντρωμένων Εφαρμογών (dApps) και του ευρύτερου κοινωνικοοικονομικού τους αντικτύπου. Η συστηματική μελέτη της εξελικτικής πορείας αυτής της τεχνολογίας καταδεικνύει, πλέον πέραν πάσης αμφιβολίας, ότι το Blockchain έχει υπερβεί οριστικά και αμετάκλητα τον αρχικό, μονοδιάστατο σχεδιασμό του, ο οποίος περιοριζόταν αποκλειστικά στη δημιουργία ενός ανθεκτικού συστήματος ψηφιακού χρήματος (peer-to-peer electronic cash), απαλλαγμένου από κεντρικό έλεγχο.

Στο αυστηρό πλαίσιο της Επιστήμης των Υπολογιστών, καταγράφεται μια ιστορική αλλαγή παραδείγματος (paradigm shift). Το οικοσύστημα έχει μετεξελιχθεί από ένα απλοϊκό σύστημα διακανονισμού συναλλαγών σε μια παγκόσμια, Turing-πλήρη, κατανεμημένη υποδομή εξυπηρετητών (global backend infrastructure). Μέσω της υλοποίησης των έξυπνων συμβολαίων, η πολύπλοκη επιχειρηματική λογική (business logic) δεν μεταφέρεται απλώς στο διαδίκτυο, αλλά κωδικοποιείται ντετερμινιστικά και εκτελείται αυτόματα από το ίδιο το δίκτυο. Η διαδικασία αυτή δημιουργεί ψηφιακά συστήματα τα οποία είναι εγγενώς διαφανή, μαθηματικά αμετάβλητα (immutable) και απόλυτα ανθεκτικά σε κάθε μορφή λογοκρισίας. Η στρατηγική αυτή μετατόπιση από τις παραδοσιακές, κεντροποιημένες σχεσιακές βάσεις δεδομένων —όπου ο διαχειριστής συστήματος (administrator) κατέχει την απόλυτη εξουσία αλλοίωσης των εγγραφών— στα δημόσια, κρυπτογραφικά ασφαλισμένα Κατανεμημένα Καθολικά (Distributed Ledgers), προσφέρει μια οριστική λύση στο διαχρονικό πρόβλημα της επίτευξης συναινετικής αλήθειας (consensus truth) σε περιβάλλοντα «μηδενικής εμπιστοσύνης» (trustless environments).

Αυτή η τεχνολογική ωρίμανση και η δημιουργία του Web 3.0 αποτέλεσαν τον καταλύτη για την εκθετική ανάπτυξη της Αποκεντρωμένης Χρηματοοικονομικής (DeFi). Η πλήρης κατάργηση των παραδοσιακών τραπεζικών στεγανών εκδημοκρατίζει την πρόσβαση σε σύνθετες χρηματοοικονομικές υπηρεσίες, όπως ο δανεισμός, η παροχή ρευστότητας και οι αυτοματοποιημένες ανταλλαγές, προωθώντας ενεργά, και όχι απλώς θεωρητικά, την παγκόσμια χρηματοοικονομική συμπερίληψη. Παράλληλα, ωστόσο, η παρούσα μελέτη ανέδειξε και αποκωδικοποίησε έναν κρίσιμο συστημικό κίνδυνο: η απουσία κεντρικών μεσαζόντων και εκκαθαριστικών οίκων μετακυλίζει εξ ολοκλήρου το βαρύτατο φορτίο της κυβερνοασφάλειας και της διαχείρισης ρίσκου στον ίδιο τον τελικό χρήστη (Self-Custody). Η αυστηρά αμετάκλητη φύση των συναλλαγών στο Blockchain (βάσει του δόγματος "code is law") σημαίνει ότι τυχόν λογικά σφάλματα στον κώδικα των εφαρμογών (smart contract exploits) ή η ελλιπής προστασία των ιδιωτικών κλειδιών, οδηγούν νομοτελειακά σε μη αναστρέψιμες οικονομικές απώλειες. Το γεγονός αυτό δημιουργεί την επιτακτική ακαδημαϊκή και βιομηχανική ανάγκη για την ανάπτυξη νέων, αποκεντρωμένων πρωτοκόλλων ασφάλισης και εργαλείων τυπικής επαλήθευσης κώδικα (formal verification).

Επιπροσθέτως, σε αμιγώς αρχιτεκτονικό επίπεδο, το λεγόμενο «Τρίλημμα του Blockchain» —η εγγενής αδυναμία ταυτόχρονης επίτευξης απόλυτης Αποκέντρωσης, μέγιστης Ασφάλειας και απεριόριστης Επεκτασιμότητας— παραμένει η μεγαλύτερη τεχνολογική πρόκληση του κλάδου. Όπως διαπιστώθηκε μέσα από την ανάλυση των σύγχρονων τοπολογιών δικτύου, η ακαδημαϊκή έρευνα στρέφεται πλέον αποκλειστικά σε Αρθρωτές Αρχιτεκτονικές (Modular Blockchains), σε λύσεις Κλίμακας Δεύτερου Επιπέδου (Layer-2 Rollups) και σε τεχνολογίες Αποδείξεων Μηδενικής Γνώσης (ZK-Proofs). Μόνο μέσω της στρατηγικής μετατόπισης του υπολογιστικού φόρτου εκτός της κύριας αλυσίδας (off-chain execution) δύναται να επιτευχθεί η βιομηχανική διαμετακομιστική ικανότητα (High TPS) που απαιτείται για την παγκόσμια υιοθέτηση, χωρίς να γίνονται εκπτώσεις στη θεμελιώδη ασφάλεια του βασικού Δικτύου (Layer 1).

Συμπερασματικά, η τεχνολογία Blockchain και τα ψηφιακά περιουσιακά στοιχεία δεν αποτελούν πλέον ένα θεωρητικό πείραμα, αλλά βρίσκονται στο κατώφλι της θεσμικής και τεχνολογικής τους ενηλικίωσης. Παρά τις τεράστιες τεχνικές, ηθικές και ρυθμιστικές προκλήσεις που αναλύθηκαν εκτενώς, η αποδεδειγμένη ικανότητα του συστήματος να λειτουργεί ως ένα αδιάβλητο, παγκόσμιο και πλήρως προγραμματιζόμενο επίπεδο μεταφοράς αξίας (Internet of Value), εγγυάται ότι θα διαδραματίσει θεμελιώδη ρόλο στην αρχιτεκτονική της επόμενης γενιάς του διαδικτύου. Το μεγάλο στοίχημα της επόμενης δεκαετίας για την επιστήμη της πληροφορικής δεν εστιάζεται πλέον αποκλειστικά στη βελτιστοποίηση του υποκείμενου κώδικα, αλλά στην

απρόσκοπτη, ασφαλή διαλειτουργικότητα αυτών των κατανεμημένων συστημάτων με τον πραγματικό κόσμο. Η τοκενοποίηση Πραγματικών Περιουσιακών Στοιχείων (RWAs), η αξιοποίηση αποκεντρωμένων χρησμών (Oracles) και η εναρμόνιση με το εξελισσόμενο παγκόσμιο κανονιστικό πλαίσιο, αποτελούν τα επόμενα ορόσημα που θα καθορίσουν την οριστική ενσωμάτωση του Web 3.0 στη σύγχρονη κοινωνία.

Πίνακας Ορολογίας

- **Αλγόριθμος Κατακερματισμού (Cryptographic Hash Function):** Μονόδρομη, ντετερμινιστική μαθηματική συνάρτηση η οποία δέχεται ως είσοδο δεδομένα οποιουδήποτε μεγέθους και παράγει μια μοναδική κρυπτογραφική συμβολοσειρά σταθερού μήκους (π.χ. 256 bits στην περίπτωση του SHA-256 ή του Keccak-256). Η κύρια ιδιότητά της είναι το «Φαινόμενο της Χιονοστιβάδας» (Avalanche Effect), όπου η παραμικρή αλλαγή στα αρχικά δεδομένα (έστω και ενός bit) μεταβάλλει ριζικά το τελικό αποτύπωμα. Λειτουργεί ως ο ακρογωνιαίος λίθος για τη διασφάλιση της ακεραιότητας των δομών (Merkle Trees) στο Blockchain, καθώς είναι υπολογιστικά ανέφικτη η εύρεση δύο διαφορετικών εισόδων που να παράγουν το ίδιο αποτύπωμα (Collision Resistance).
- **Αποκεντρωμένη Εφαρμογή (dApp - Decentralized Application):** Αρχιτεκτονική λογισμικού νέας γενιάς (Web 3.0), στην οποία το λογικό πλαίσιο (backend) δεν εκτελείται σε κεντρικούς διακομιστές υπολογιστικού νέφους (π.χ. AWS), αλλά φιλοξενείται σε ένα δημόσιο, ομότιμο δίκτυο (P2P). Η επιχειρησιακή λογική της εφαρμογής κωδικοποιείται αποκλειστικά μέσω Έξυπνων Συμβολαίων (Smart Contracts). Οι dApps είναι εγγενώς ανθεκτικές στη λογοκρισία (censorship-resistant) και επιτρέπουν στους χρήστες να αλληλεπιδρούν μαζί τους διατηρώντας την πλήρη αυτο-φύλαξη (self-custody) των κεφαλαίων τους.
- **Διπλή Δαπάνη (Double Spending Problem):** Το θεμελιώδες συστημικό ελάττωμα των αμιγώς ψηφιακών, αποκεντρωμένων νομισμάτων πριν από την έλευση του Bitcoin. Πρόκειται για τον θεωρητικό κίνδυνο ένας χρήστης να αντιγράψει τα δεδομένα ενός ψηφιακού περιουσιακού στοιχείου και να ξοδέψει το ίδιο νόμισμα ταυτόχρονα σε δύο διαφορετικούς παραλήπτες. Το Blockchain επιλύει οριστικά αυτό το πρόβλημα συνδυάζοντας την κρυπτογραφική χρονοσήμανση (Timestamping) με έναν αποκεντρωμένο Αλγόριθμο Συναίνεσης (Nakamoto Consensus), διασφαλίζοντας ότι ολόκληρο το δίκτυο συμφωνεί για την απόλυτη χρονολογική σειρά των μεταφορών αξίας.
- **Έξυπνο Συμβόλαιο (Smart Contract):** Αυτοεκτελούμενος, αμετάβλητος (immutable) προγραμματιστικός κώδικας (συνήα γραμμένος σε γλώσσες όπως η Solidity), ο οποίος αναπτύσσεται (deployed) και αποθηκεύεται μόνιμα στο Blockchain. Λειτουργεί ως μια αποκεντρωμένη μηχανή καταστάσεων (state machine): μόλις πληρωθούν συγκεκριμένες, εκ των προτέρων καθορισμένες και μαθηματικά επαληθεύσιμες συνθήκες (If-This-Then-That), το συμβόλαιο εκτελεί τις εντολές αυτόματα (π.χ. μεταφορά κεφαλαίων ή έκδοση τίτλων), δίχως τη δυνατότητα ανθρώπινης παρέμβασης, ακύρωσης ή διαμεσολάβησης από τρίτα μέρη.
- **Ιδιωτικό Κλειδί (Private Key):** Μια κρυπτογραφική μεταβλητή ύψιστης ασφαλείας, η οποία λαμβάνει τη μορφή ενός τεράστιου, τυχαία παραγόμενου ακέραιου αριθμού (Εντροπία 256-bit). Βάσει της Ασύμμετρης Κρυπτογραφίας Ελλειπτικών Καμπυλών (ECC), το κλειδί αυτό χρησιμοποιείται για την παραγωγή Ψηφιακών Υπογραφών (Digital Signatures). Οι υπογραφές αυτές αποτελούν τη μοναδική μαθηματική απόδειξη που εξουσιοδοτεί αμετάκλητα την κίνηση των νομισμάτων από μια διεύθυνση. Η απώλεια ή η διαρροή του Ιδιωτικού Κλειδιού συνεπάγεται την άμεση και οριστική απώλεια του συνόλου των ψηφιακών περιουσιακών στοιχείων.
- **Κόμβος (Node):** Οποιαδήποτε ανεξάρτητη υπολογιστική μονάδα είναι συνδεδεμένη στο ομότιμο δίκτυο (P2P network) του Blockchain. Οι "Πλήρεις Κόμβοι" (Full Nodes) διατηρούν ένα κρυπτογραφικά επαληθευμένο, ιστορικό αντίγραφο ολόκληρου του Καθολικού (Ledger) από τη στιγμή της δημιουργίας του. Ο ρόλος τους είναι κρίσιμος, καθώς ελέγχουν αυστηρά (validate) κάθε νέα συναλλαγή και κάθε νέο μπλοκ απέναντι στους κανόνες συναίνεσης του δικτύου (consensus rules), απορρίπτοντας αυτόματα οποιαδήποτε προσπάθεια αλλοίωσης ή πλαστογραφίας από κακόβουλους δρώντες.
- **Μπλοκ Γένεσης (Genesis Block):** Το απόλυτο θεμέλιο κάθε δικτύου Blockchain. Αποτελεί το πρώτο μπλοκ (Block 0) που καταγράφεται ποτέ στην αλυσίδα. Σε αντίθεση με όλα τα μεταγενέστερα μπλοκ, δεν περιέχει τον κρυπτογραφικό δείκτη (previous hash) κάποιου προηγούμενου μπλοκ.
- **Φράση Ανάκτησης (Seed Phrase / Mnemonic Phrase):** Πρότυπο βιομηχανίας (BIP-39) που γεφυρώνει τη μηχανική κρυπτογραφία με την ανθρώπινη μνήμη. Πρόκειται για

τη μετατροπή της ακατέργαστης τυχαιότητας ενός πορτοφολιού σε μια αναγνώσιμη ακολουθία 12 ή 24 προκαθορισμένων αγγλικών λέξεων. Μέσω ισχυρών συναρτήσεων παραγωγής κλειδιών (όπως η PBKDF2), η φράση αυτή λειτουργεί ως ο «Κύριος Σπόρος» (Master Seed).

Πίνακας Συντμήσεων - Ακρωνυμίων

- **AML (Anti-Money Laundering):** Καταπολέμηση της Νομιμοποίησης Εσόδων από Παράνομες Δραστηριότητες (Κανονιστικό πλαίσιο).
- **AMM (Automated Market Maker):** Αυτοματοποιημένος Ειδικός Διαπραγματευτής (Αλγοριθμικός μηχανισμός παροχής ρευστότητας σε αποκεντρωμένα δίκτυα).
- **CEX (Centralized Exchange):** Κεντριοποιημένο Ανταλλακτήριο Κρυπτονομισμάτων (Πλατφόρμα ανταλλαγής με κεντρικό θεματοφύλακα).
- **DeFi (Decentralized Finance):** Αποκεντρωμένη Χρηματοοικονομική (Οικοσύστημα χρηματοοικονομικών εφαρμογών ανοιχτού κώδικα).
- **DEX (Decentralized Exchange):** Αποκεντρωμένο Ανταλλακτήριο (Πρωτόκολλο ανταλλαγής ψηφιακών στοιχείων χωρίς μεσάζοντες).
- **EVM (Ethereum Virtual Machine):** Εικονική Μηχανή του Ethereum (Το αποκεντρωμένο περιβάλλον εκτέλεσης των έξυπνων συμβολαίων).
- **KYC (Know Your Customer):** Διαδικασία Ταυτοποίησης Πελατών (Υποχρεωτική διαδικασία ελέγχου πραγματικής ταυτότητας χρήστη).
- **NFT (Non-Fungible Token):** Μη-Ανταλλάξιμο Ψηφιακό Στοιχείο / Κρυπτογραφικό Μάρκο (Απόδειξη μοναδικής ψηφιακής ιδιοκτησίας).
- **P2P (Peer-to-Peer):** Ομότιμο Δίκτυο (Αρχιτεκτονική καταμεμημένου δικτύου υπολογιστών χωρίς κεντρικό διακομιστή).
- **PoS (Proof of Stake):** Απόδειξη Συμμετοχής (Αλγόριθμος αποκεντρωμένης συναίνεσης βασισμένος στην οικονομική δέσμευση κεφαλαίων).
- **PoW (Proof of Work):** Απόδειξη Εργασίας (Αλγόριθμος αποκεντρωμένης συναίνεσης βασισμένος στην κατανάλωση υπολογιστικής ισχύος).
- **TPS (Transactions Per Second):** Συναλλαγές ανά Δευτερόλεπτο (Βασική μετρική αξιολόγησης της διαμετακομιστικής ικανότητας και κλιμάκωσης ενός δικτύου).

BIBΛΙΟΓΡΑΦΙΑ (REFERENCES)

1. **S. Nakamoto**, "Bitcoin: A Peer-to-Peer Electronic Cash System," Decentralized Business Review, 2008.
2. **V. Buterin**, "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum White Paper, 2014.
3. **G. Wood**, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," Ethereum Project Yellow Paper, vol. 151, 2014.
4. **L. Lamport, R. Shostak, and M. Pease**, "The Byzantine Generals Problem," ACM Transactions on Programming Languages and Systems (TOPLAS), vol. 4, no. 3, pp. 382-401, 1982.
5. **D. Chaum**, "Blind Signatures for Untraceable Payments," in Advances in Cryptology, Springer, 1983, pp. 199-203.
6. **A. Back**, "Hashcash - A Denial of Service Counter-Measure," Original Technical Report, 2002.
7. **N. Szabo**, "Smart Contracts: Building Blocks for Digital Markets," EXTROPY: The Journal of Transhumanist Thought, no. 16, 1996.
8. **W. Dai**, "b-money," 1998. [Online]. Available: <http://www.weidai.com/bmoney.txt>.
9. **T. May**, "The Crypto Anarchist Manifesto," High Noon on the Electronic Frontier, pp. 41-44, 1992.
10. **E. Hughes**, "A Cypherpunk's Manifesto," 1993.
11. **A. M. Antonopoulos**, Mastering Bitcoin: Programming the Open Blockchain, 2nd ed. Sebastopol, CA, USA: O'Reilly Media, 2017.
12. **R. C. Merkle**, "A Digital Signature Based on a Conventional Encryption Function," in Advances in Cryptology — CRYPTO '87, Springer, 1988, pp. 369-378.
13. **S. Böhme, N. Christin, B. Edelman, and T. Moore**, "Bitcoin: Economics, Technology, and Governance," Journal of Economic Perspectives, vol. 29, no. 2, pp. 213-238, 2015.
14. **M. Castro and B. Liskov**, "Practical Byzantine Fault Tolerance," in Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI), 1999, pp. 173-186.
15. **Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang**, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in 2017 IEEE International Congress on Big Data, 2017, pp. 557-564.
16. **Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou**, "A Survey of Distributed Consensus Protocols for Blockchain Networks," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1432-1465, 2020.
17. **J. Garay, A. Kiayias, and N. Leonardos**, "The Bitcoin Backbone Protocol: Analysis and Applications," EUROCRYPT, Springer, 2015, pp. 281-310.
18. **A. M. Antonopoulos and G. Wood**, Mastering Ethereum: Building Smart Contracts and DApps, Sebastopol, CA, USA: O'Reilly Media, 2018.
19. **K. Delmolino, M. Arnett, A. Kosba, A. Miller, and E. Shi**, "Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab," in Financial Cryptography and Data Security, Springer, 2016, pp. 79-94.
20. **N. Atzei, M. Bartoletti, and T. Cimoli**, "A Survey of Attacks on Ethereum Smart Contracts (SoK)," in POST, Springer, 2017, pp. 164-186.
21. **L. Luu, D. H. Chu, H. Olickel, P. Saxena, and A. Hobor**, "Making Smart Contracts Smarter," in Proceedings of the 2016 ACM SIGSAC Conference, 2016, pp. 254-269.
22. **F. Vogelsteller and V. Buterin**, "ERC-20 Token Standard," Ethereum Improvement Proposals, no. 20, 2015.
23. **F. Schär**, "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets," Federal Reserve Bank of St. Louis Review, vol. 103, no. 2, pp. 153-174, 2021.
24. **W. Warren and A. Bandeau**, "0x: An Open Protocol for Decentralized Exchange on the

- Ethereum Blockchain," 2017.
25. **H. Adams, N. Zinsmeister, M. Salem, R. Keefer, and D. Robinson**, "Uniswap v3 Core," 2021.
 26. **S. M. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. J. Knottenbelt**, "SoK: Decentralized Finance (DeFi)," in AFT, 2021.
 27. **R. Leshner and G. Hayes**, "Compound: The Money Market Protocol," 2019.
 28. **J. Z. Zhang, K. Zhong, J. Ding, et al.**, "Automated Market Makers: A Theoretical Overview," IEEE Access, vol. 9, pp. 142345-142358, 2021.
 29. **World Bank Group**, "The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19," Washington, DC, 2022.
 30. **Chainanalysis**, "The 2025 Crypto Crime Report," Chainanalysis Research, 2025.
 31. **D. Yermack**, "Is Bitcoin a Real Currency? An Economic Appraisal," in Handbook of Digital Currency, Elsevier, 2015, pp. 31-43.
 32. **A. M. Antonopoulos**, The Internet of Money, Merkle Bloom LLC, 2016.
 33. **P. Daian et al.**, "Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability," in IEEE Symposium on Security and Privacy (SP), 2020, pp. 910-927.
 34. **K. Wüst and A. Gervais**, "Do you need a Blockchain?," in CVCBT, IEEE, 2018, pp. 45-54.
 35. **E. W. K. Tsang**, "The Blockchain Trilemma," Journal of Digital Economy, vol. 1, no. 1, pp. 11-20, 2022.
 36. **V. Buterin**, "A rollup-centric ethereum roadmap," Ethereum Foundation Blog, 2020.
 37. **H. Kalodner et al.**, "Arbitrum: Scalable, private smart contracts," in 27th USENIX Security Symposium, 2018, pp. 1353-1370.
 38. **E. Ben-Sasson et al.**, "StarkNet Whitepaper," StarkWare Industries, 2021.
 39. **K. J. Gogol et al.**, "A comprehensive survey of Layer 2 scaling solutions," IEEE Access, vol. 10, pp. 45312-45330, 2022.
 40. **M. Al-Bassam, A. Sonnino, and V. Buterin**, "LazyLedger: A Distributed Data Availability Ledger With Client-Side Smart Contracts," arXiv preprint arXiv:1905.09274, 2019.
 41. **J. Adler et al.**, "Celestia: A scalable general-purpose data availability layer," Celestia Whitepaper, 2022.
 42. **V. Buterin et al.**, "EIP-4844: Shard Blob Transactions," Ethereum Improvement Proposals, 2022.
 43. **J. Poon and T. Dryja**, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments," Working Paper, 2016.
 44. **G. Wood**, "Polkadot: Vision for a heterogeneous multi-chain framework," Whitepaper, 2016.
 45. **J. Kwon and E. Buchman**, "Cosmos: A Network of Distributed Ledgers," Cosmos Whitepaper, 2019.
 46. **S. Sayeed, H. Marco-Gisbert, and T. Caira**, "Smart contract vulnerabilities: A systematic review," IEEE Access, vol. 8, pp. 114532-114550, 2020.
 47. **D. Perez and B. Livshits**, "Smart contract vulnerabilities: Vulnerability sources and security patterns," arXiv preprint arXiv:1908.08605, 2021.
 48. **P. Tolmachev et al.**, "A survey of smart contract formal verification tools," ACM Computing Surveys (CSUR), vol. 54, no. 7, pp. 1-38, 2021.
 49. **T. Chen et al.**, "Understanding Ethereum via Graph Analysis," in IEEE INFOCOM 2018, pp. 1484-1492.
 50. **A. Ferreira**, "Solidity Smart Contracts: Design Patterns and Security," Journal of Systems Architecture, vol. 115, 102008, 2021.
 51. **ConsenSys**, "Ethereum Smart Contract Security Best Practices," ConsenSys Diligence, 2022.

52. **I. Sergey and A. Hobor**, "A concurrent perspective on smart contracts," in International Conference on Financial Cryptography and Data Security, Springer, 2017.
53. **M. Bartoletti and L. Pompianu**, "An empirical analysis of smart contracts: platforms, applications, and design patterns," in International Conference on Financial Cryptography, 2017.
54. **K. Wüst and A. Gervais**, "Ethereum Smart Contract Security," ETH Zurich Research Report, 2019.
55. **OpenZeppelin**, "OpenZeppelin Contracts: A library for secure smart contract development," 2021.
56. **S. Loesch et al.**, "Impermanent loss in uniswap v3," arXiv preprint arXiv:2111.09192, 2021.
57. **L. Gudgeon et al.**, "The decentralized financial crisis: Attacking DeFi protocols via flash loans," arXiv preprint arXiv:2002.08099, 2020.
58. **K. Qin et al.**, "Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit," in Financial Cryptography and Data Security, Springer, 2021.
59. **A. Ellis, A. Juels, and S. Nazarov**, "ChainLink: A Decentralized Oracle Network," SmartContract ChainLink Ltd., 2017.
60. **L. Breidenbach et al.**, "Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks," Chainlink Labs, 2021.
61. **J. Wang, S. Hu, and Y. Liu**, "A Survey on Decentralized Finance (DeFi) Security: Vulnerabilities, Attacks, and Defenses," arXiv preprint arXiv:2108.13014, 2021.
62. **G. Caldarelli**, "Understanding the blockchain oracle problem: A call for action," Information, vol. 11, no. 11, 509, 2020.
63. **K. Qin et al.**, "CeFi vs. DeFi – Comparing Centralized to Decentralized Finance," arXiv preprint arXiv:2106.08195, 2021.
64. **Aave Protocol**, "Aave V2 Whitepaper," Aave.com, 2020.
65. **Y. K. Wang**, "Automated Market Makers for Decentralized Exchanges," Journal of Financial Technology, vol. 5, no. 2, 2022.
66. **Citigroup**, "Money, Tokens, and Games: Blockchain's Next Billion Users and Trillions in Value," Citi Global Perspectives & Solutions, 2023.
67. **European Commission**, "Regulation on Markets in Crypto-assets (MiCA)," COM(2020) 593 final, Brussels, 2020.
68. **D. A. Zetzsche et al.**, "The Markets in Crypto-Assets Regulation (MiCA) and the EU Digital Finance Strategy," Capital Markets Law Journal, vol. 16, no. 2, pp. 203-225, 2021.
69. **Bank for International Settlements (BIS)**, "Central bank digital currencies: foundational principles and core features," BIS Report, 2020.
70. **R. Auer and R. Böhme**, "The technology of retail central bank digital currency," BIS Quarterly Review, 2020.
71. **European Central Bank (ECB)**, "Report on the investigation phase of the digital euro," ECB Publications, 2023.
72. **T. Bamert, C. Decker, and R. Wattenhofer**, "BlueMatador: A tokenization framework for Real World Assets," Crypto Valley Research, 2022.
73. **Centrifuge**, "Real World Assets: Bridging DeFi and Traditional Finance," Centrifuge Protocol Documentation, 2022.
74. **J. Camier, M. Pieters, and L. Schilte**, "ERC-3643: T-REX - Token for Regulated Exchanges," Ethereum Improvement Proposals, 2021.
75. **OECD**, "The Tokenisation of Assets and Potential Implications for Financial Markets," OECD Blockchain Policy Series, 2023.
76. **W3C**, "Decentralized Identifiers (DIDs) v1.0," World Wide Web Consortium Recommendation, 2022.
77. **W3C**, "Verifiable Credentials Data Model v1.1," World Wide Web Consortium Recommendation, 2022.

78. **E. G. Weyl, P. Ohlhaber, and V. Buterin**, "Decentralized Society: Finding Web3's Soul," SSRN Electronic Journal, 2022.
79. **Messari Research**, "The DePIN Sector Map: Decentralized Physical Infrastructure Networks," Messari Report, 2023.
80. **H. Chen, S. Liu, and J. Wu**, "Decentralized Physical Infrastructure Networks (DePIN): Concepts, Architectures, and Open Challenges," IEEE Internet of Things Journal, 2023.
81. **V. Buterin**, "The promise and challenges of crypto + AI applications," Vitalik.ca, 2024.
82. **M. Ali, J. Nelson, and R. Shea**, "The Convergence of Artificial Intelligence and Blockchain Technology," IEEE Network, vol. 36, no. 1, pp. 14-20, 2022.
83. **J. Li, K. Zhang, and X. Wang**, "A Survey of Zero-Knowledge Machine Learning (zkML)," arXiv preprint arXiv:2308.01234, 2023.
84. **V. Buterin, Y. Huang, and T. Beiko**, "ERC-4337: Account Abstraction Using Alt Mempool," Ethereum Improvement Proposals, 2021.
85. **Paradigm**, "Intent-Based Architectures and their Risks," Paradigm Research, 2023.
86. **M. Fernandez-Carames and P. Fraga-Lamas**, "Towards Post-Quantum Blockchain: A Review on Cyberattacks and Defense Strategies," IEEE Access, vol. 8, pp. 21091-21116, 2020.
87. **D. Aggarwal et al.**, "Quantum attacks on Bitcoin, and how to protect against them," Ledger, vol. 3, 2018.
88. **L. Chen et al.**, "Report on Post-Quantum Cryptography," NIST Interagency Report 8105, 2016.
89. **NIST**, "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms," NIST News Release, 2022.
90. **E. Ben-Sasson et al.**, "Scalable, transparent, and post-quantum secure computational integrity," IACR Cryptology ePrint Archive, 2018.
91. **S. Bowe, J. Grigg, and D. Hopwood**, "Halo 2: recursive proof composition without a trusted setup," Electronic Colloquium on Computational Complexity, 2020.
92. **J. Feist and F. Dankrad**, "KZG Polynomial Commitments," Ethereum Research, 2023.
93. **D. Moher et al.**, "Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement," PLoS medicine, vol. 6, no. 7, 2009.
94. **B. Kitchenham**, "Procedures for performing systematic reviews," Keele University Technical Report, 2004.
95. **A. Liberati et al.**, "The PRISMA statement for reporting systematic reviews and meta-analyses," BMJ, vol. 339, 2009.
96. **K. Petersen et al.**, "Systematic mapping studies in software engineering," in 12th International Conference on Evaluation and Assessment in Software Engineering, 2008.
97. **M. Petticrew and H. Roberts**, Systematic reviews in the social sciences: A practical guide, Blackwell Publishing, 2006.
98. **C. Wohlin et al.**, Experimentation in software engineering, Springer Science & Business Media, 2012.
99. **Y. Levy and T. J. Ellis**, "A systems approach to conduct an effective literature review in support of information systems research," Informing Science Journal, vol. 9, 2006.
100. **H. Snyder**, "Literature review as a research methodology: An overview and guidelines," Journal of Business Research, vol. 104, pp. 333-339, 2019.

Παράρτημα Α: Πηγαίος Κώδικας Υλοποίησης Αποκεντρωμένου Πρωτοκόλλου Δανεισμού (DeFi Lending Smart Contract)

Στο παρόν παράρτημα παρατίθεται ο πλήρης πηγαίος κώδικας (γραμμένος στη γλώσσα προγραμματισμού Solidity) ενός ενδεικτικού Έξυπνου Συμβολαίου για τη λειτουργία ενός Αποκεντρωμένου Πρωτοκόλλου Δανεισμού. Το συμβόλαιο ακολουθεί τη βασική επιχειρηματική λογική του DeFi, επιτρέποντας στους χρήστες να καταθέτουν ψηφιακά περιουσιακά στοιχεία ως ρευστότητα (Liquidity Providers) και να δανείζονται κεφάλαια έναντι ενεχύρου (Collateralized Borrowing).

Ο κώδικας ενσωματώνει σημαντικούς ελέγχους κυβερνοασφάλειας, όπως προστασία από επιθέσεις επαναεισόδου (Reentrancy Guard), ελέγχους υπερχειλίσης μέσω της βιβλιοθήκης SafeMath (εγγενής πλέον στις νεότερες εκδόσεις του compiler), και αυστηρή διαχείριση καταστάσεων μέσω modifiers. // SPDX-License Identifier: MIT

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
/**
 * @title Decentralized Lending Protocol (DeFi)
 * @author Ιωάννης Μπαλκούρας - Πτυχιική Εργασία
 * @notice Ένα πλήρες έξυπνο συμβόλαιο για καταθέσεις, δανεισμό και
 ρευστοποίηση ψηφιακών περιουσιακών στοιχείων (ETH).
 * @dev Περιλαμβάνει μηχανισμούς ασφάλειας κατά των επιθέσεων
 Reentrancy.
 */
contract DeFiLendingProtocol {
    // --- Καταστάσεις και Μεταβλητές (State Variables) ---

    // Η διεύθυνση του δημιουργού/διαχειριστή του συμβολαίου
    address public owner;

    // Ποσοστό επιτοκίου (π.χ., 5% ετησίως)
    uint256 public constant INTEREST_RATE = 5;

    // Απαιτούμενο ποσοστό υπερ-εξασφάλισης (Over-collateralization
 ratio).
    // Παράδειγμα: 150 σημαίνει ότι για κάθε 100 νομίσματα δανείου,
 απαιτούνται 150 ως ενέχυρο.
    uint256 public constant COLLATERAL_RATIO = 150;

    // Ποσοστό έκπτωσης κατά τη ρευστοποίηση (Liquidation Penalty)
    uint256 public constant LIQUIDATION_PENALTY = 10; // 10%
    // --- Δομές Δεδομένων (Structs) ---

    // Δομή που αποθηκεύει τα δεδομένα του κάθε χρήστη
 (δανειολήπτη/καταθέτη)
    struct UserAccount {
        uint256 depositedCollateral; // Ποσό ενεχύρου που έχει κατατεθεί
        uint256 borrowedAmount; // Ποσό που έχει δανειστεί
        uint256 lastInterestUpdate; // Χρονοσφραγίδα (timestamp) της
 τελευταίας ενημέρωσης τόκων
    }
```

```
// Χαρτογράφηση (Mapping) για τη σύνδεση κάθε διεύθυνσης χρήστη με
το λογαριασμό του
mapping(address => UserAccount) public accounts;

// --- Ασφάλεια: Προστασία από Reentrancy ---
// Μεταβλητή ελέγχου για τον modifier nonReentrant
bool private locked;

// --- Γεγονότα (Events) ---
// Τα γεγονότα επιτρέπουν στις off-chain εφαρμογές
(frontend/backend) να ενημερώνονται για τις αλλαγές στο blockchain.
event CollateralDeposited(address indexed user, uint256 amount);
event CollateralWithdrawn(address indexed user, uint256 amount);
event Borrowed(address indexed user, uint256 amount);
event Repaid(address indexed user, uint256 amount);
event Liquidated(address indexed liquidator, address indexed user,
uint256 penaltyAmount);

// --- Τροποποιητές (Modifiers) ---

/**
 * @dev Αποτρέπει τις επιθέσεις επαναισόδου (Reentrancy Attacks)
κλειδώνοντας την κατάσταση του συμβολαίου.
 */
modifier nonReentrant() {
    require(!locked, "Reentrant call detected!");
    locked = true;
    _;
    locked = false;
}

/**
 * @dev Περιορίζει την πρόσβαση σε συγκεκριμένες λειτουργίες μόνο
στον διαχειριστή.
 */
modifier onlyOwner() {
    require(msg.sender == owner, "Unauthorized: Caller is not the
owner.");
    _;
}

// --- Κατασκευαστής (Constructor) ---
constructor() {
    owner = msg.sender;
}

// --- Βασικές Λειτουργίες Πρωτοκόλλου (Core Functions) ---
/**
 * @notice Κατάθεση κρυπτονομίσματος (ETH) ως ενέχυρο από τον χρήστη.
 * @dev Η συνάρτηση είναι 'payable' ώστε να δέχεται το ETH που
στέλνει ο χρήστης.
 */
```

```
function depositCollateral() external payable nonReentrant {
    require(msg.value > 0, "Deposit amount must be greater than
zero.");
    // Ενημέρωση του υπολοίπου ενεχύρου του χρήστη
    accounts[msg.sender].depositedCollateral += msg.value;

    // Αρχικοποίηση της χρονοσφραγίδας αν είναι η πρώτη κατάθεση
    if (accounts[msg.sender].lastInterestUpdate == 0) {
        accounts[msg.sender].lastInterestUpdate = block.timestamp;
    }
    // Εκπομπή γεγονότος για το frontend/backend
    emit CollateralDeposited(msg.sender, msg.value);
}
/**
 * @notice Δανεισμός κεφαλαίων έναντι του ενεχύρου που έχει
κατατεθεί.
 * @param borrowAmount Το ποσό που επιθυμεί να δανειστεί ο χρήστης.
 * @dev Ελέγχει την αναλογία υπερ-εξασφάλισης (Over-
collateralization) πριν εγκρίνει το δάνειο.
 */
function borrow(uint256 borrowAmount) external nonReentrant {
    require(borrowAmount > 0, "Borrow amount must be greater than
zero.");

    // Φόρτωση των δεδομένων του χρήστη στη μνήμη (memory) για
εξοικονόμηση αερίου (gas)
    UserAccount memory user = accounts[msg.sender];

    require(user.depositedCollateral > 0, "No collateral
deposited.");
    // Υπολογισμός του μέγιστου επιτρεπτού δανείου βάσει του
Collateral Ratio (150%)
    // Μαθηματικός τύπος: Max Borrow = (Collateral * 100) / 150
    uint256 maxBorrowable = (user.depositedCollateral * 100) /
COLLATERAL_RATIO;

    // Ο χρήστης δεν μπορεί να δανειστεί περισσότερα από όσα του
επιτρέπει το ενέχυρό του
    require(user.borrowedAmount + borrowAmount <= maxBorrowable,
"Insufficient collateral to borrow this amount.");

    // Βεβαίωση ότι το συμβόλαιο διαθέτει επαρκή ρευστότητα για να
δώσει το δάνειο
    require(address(this).balance >= borrowAmount, "Protocol lacks
sufficient liquidity.");
    // --- Ενημέρωση Κατάστασης (State Changes) ---
    // Σύμφωνα με το πρότυπο Checks-Effects-Interactions,
ενημερώνουμε πρώτα την κατάσταση
```

```

        accounts[msg.sender].borrowedAmount += borrowAmount;

        // --- Αλληλεπίδραση (Interaction) ---
        // Αποστολή των κεφαλαίων στον χρήστη
        (bool success, ) = payable(msg.sender).call{value:
borrowAmount}("");
        require(success, "Transfer failed.");
        emit Borrowed(msg.sender, borrowAmount);
    }
    // --- Αποπληρωμή και Διαχείριση Ρίσκου (Repayment & Liquidation) ---
    /**
     * @notice Εσωτερική συνάρτηση για τον υπολογισμό των συσσωρευμένων
τόκων.
     * @param userAddress Η διεύθυνση του δανειολήπτη.
     * @return 0 τόκος που έχει συσσωρευτεί με βάση το χρόνο που έχει
παρέλθει.
     */
    function calculateInterest(address userAddress) internal view
returns (uint256) {
        UserAccount memory user = accounts[userAddress];
        if (user.borrowedAmount == 0) return 0;
        uint256 timeElapsed = block.timestamp - user.lastInterestUpdate;

        // Απλός υπολογισμός τόκου (Simple Interest)
        // (Δάνειο * Επιτόκιο * Χρόνος) / (100 * 31536000 δευτερόλεπτα
το χρόνο)
        uint256 interest = (user.borrowedAmount * INTEREST_RATE *
timeElapsed) / (100 * 365 days);
        return interest;
    }
    /**
     * @notice Αποπληρωμή του δανείου και των τόκων.
     * @dev Μετά την πλήρη αποπληρωμή, ο χρήστης μπορεί να αποσύρει το
ενέχυρό του.
     */
    function repay() external payable nonReentrant {
        UserAccount storage user = accounts[msg.sender];
        require(user.borrowedAmount > 0, "No active loan to repay.");
        uint256 accruedInterest = calculateInterest(msg.sender);
        uint256 totalDebt = user.borrowedAmount + accruedInterest;

        require(msg.value >= totalDebt, "Insufficient amount to repay
full debt.");
        // Μηδενισμός του χρέους
        user.borrowedAmount = 0;
        user.lastInterestUpdate = block.timestamp; // Ενημέρωση
χρονοσφραγίδας

```

```

        // Επιστροφή τυχόν ρέστων (над-πληρωμή)
        if (msg.value > totalDebt) {
            uint256 refund = msg.value - totalDebt;
            (bool success, ) = payable(msg.sender).call{value:
refund}("");
            require(success, "Refund failed.");
        }
        emit Repaid(msg.sender, totalDebt);
    }
    /**
     * @notice Ρευστοποίηση ενός λογαριασμού που δεν καλύπτεται επαρκώς
(Under-collateralized).
     * @param targetUser Η διεύθυνση του χρήστη προς ρευστοποίηση.
     * @dev Οποιοσδήποτε χρήστης μπορεί να καλέσει αυτή τη συνάρτηση για
να προστατεύσει το πρωτόκολλο,
     * λαμβάνοντας ως ανταμοιβή (liquidation penalty) ένα μέρος του
ενεχύρου.
     */
    function liquidate(address targetUser) external nonReentrant {
        UserAccount storage target = accounts[targetUser];
        require(target.borrowedAmount > 0, "Target has no active
loan.");
        uint256 totalDebt = target.borrowedAmount +
calculateInterest(targetUser);
        uint256 currentCollateral = target.depositedCollateral;
        // Έλεγχος αν ο χρήστης βρίσκεται όντως κάτω από το όριο (Under-
collateralized)
        // Αν το (Ενέχυρο * 100) / Χρέος είναι μικρότερο από το 150%,
τότε κινδυνεύει!
        require((currentCollateral * 100) / totalDebt <
COLLATERAL_RATIO, "Account is sufficiently collateralized.");
        // Υπολογισμός της ποινής (penalty) που θα κρατήσει το πρωτόκολλο
/ liquidator
        uint256 penalty = (totalDebt * LIQUIDATION_PENALTY) / 100;
        uint256 totalDeduction = totalDebt + penalty;
        // Βεβαιωνόμαστε ότι το ενέχυρο φτάνει να καλύψει το χρέος και
την ποινή
        require(currentCollateral >= totalDeduction, "Bad debt:
Collateral cannot cover debt and penalty.");
        // Αφαίρεση του χρέους και της ποινής από το ενέχυρο του χρήστη
        target.depositedCollateral -= totalDeduction;
        target.borrowedAmount = 0; // Το χρέος θεωρείται ξοφλημένο
        // Το ποσό του χρέους (totalDebt) μένει στο πρωτόκολλο για να
αναπληρώσει τη ρευστότητα.
        // Η ποινή (penalty) αποστέλλεται στον χρήστη (liquidator) που
κάλεσε τη συνάρτηση ως κίνητρο.
        (bool success, ) = payable(msg.sender).call{value: penalty}("");
        require(success, "Penalty transfer failed.");
    }

```

```
        emit Liquidated(msg.sender, targetUser, penalty);  
    }  
} // Τέλος του Smart Contract
```