

Αποκεντρωμένο Δίκτυο Φήμης: Ένα Πλαίσιο για τη Φυσική Οργάνωση της Κοινωνίας

Pavel Kudrna
Prague, Czechia
Draft v1 — March 2026

Abstract

Η αίσθηση της δικαιοσύνης—η πεποίθηση ότι τα άδικα διορθώνονται και η αξία ανταμείβεται—είναι η ισχυρότερη συνεκτική δύναμη της κοινωνίας. Όταν οι κεντριοποιημένοι θεσμοί διακυβέρνησης δεν μπορούν να προσφέρουν αυτήν την αίσθηση, επειδή το κόστος επιβολής ενός δικαιώματος υπερβαίνει την αξία του ίδιου του δικαιώματος, η κοινωνική συνοχή διαβρώνεται. Οι σημερινές θεσμικές δομές αποτυγχάνουν να επιλύσουν μια σημαντική κατηγορία διαφορών με συστηματικά τον ίδιο τρόπο που ο κεντρικός σχεδιασμός αποτυγχάνει να καταναείμει τους πόρους: μέσω ασυμμετρίας πληροφόρησης, ελλείποντων βρόχων ανάδρασης και αποσύνδεσης των υπευθύνων λήψης αποφάσεων από τις συνέπειες των αποφάσεών τους. Η παρούσα εργασία παρουσιάζει ένα Κοινωνικό Δίκτυο Φήμης (Reputation Social Network, RSN): ένα αποκεντρωμένο, αδιάφθορο, ανθεκτικό στη λογοκρισία επίπεδο επικοινωνίας που βασίζεται σε Αποκεντρωμένα Αναγνωριστικά (Decentralized Identifiers, DIDs) και επιτρέπει σε ψευδώνυμους συμμετέχοντες να δημοσιεύουν, να επαληθεύουν και να καταναλώνουν πληροφορίες φήμης σχετικά με τη συμπεριφορά στον πραγματικό κόσμο. Ο βασικός μηχανισμός στηρίζεται σε τρεις αρχές σχεδιασμού: (1) μια ασύμμετρη δομή κόστους όπου η ανάγνωση δεδομένων φήμης είναι φθηνή, αλλά η εγγραφή απαιτεί επαληθεύσιμη προσπάθεια· (2) ένα μη ντετερμινιστικό πρωτόκολλο επιλογής επαληθευτή βασισμένο σε συνεπή κατακερματισμό (consistent hashing) που τιμολογεί τους ριζοσπαστικούς ισχυρισμούς μέσω κλιμακούμενου κόστους επανάληψης· και (3) ένα μοντέλο αρχής φήμης καθοδηγούμενο από την αγορά, όπου ιδιωτικοί επαληθευτές διακινδυνεύουν τη συσσωρευμένη φήμη τους στην ακρίβεια των ισχυρισμών που εγκρίνουν. Η προκύπτουσα αρχιτεκτονική παράγει αναδυόμενη αξιοκρατία χωρίς κεντρικό συντονισμό και επιτρέπει μια σταδιακή, αναστρέψιμη διαδρομή μετάβασης από τα υπάρχοντα κρατικά συστήματα.

1 Εισαγωγή

1.1 Το Πρόβλημα της Κεντριοποιημένης Εμπιστοσύνης

Η σύγχρονη διακυβέρνηση στηρίζεται σε μια θεμελιώδη παραδοχή: ότι οι κεντριοποιημένοι θεσμοί μπορούν να διαμεσολαβούν την εμπιστοσύνη μεταξύ αγνώστων σε μεγάλη κλίμακα. Τα δικαστήρια εκδικάζουν διαφορές. Τα μητρώα πιστοποιούν την ιδιοκτησία. Οι ρυθμιστικές αρχές επιβάλλουν πρότυπα. Αυτοί οι θεσμοί σχεδιάστηκαν σε μια εποχή όπου η πληροφορία ήταν σπάνια, η επικοινωνία αργή, και η ανάθεση εξουσίας σε ένα κεντρικό όργανο ήταν ο μόνος εφικτός μηχανισμός συντονισμού. Η κεντριοποιημένη διακυβέρνηση, ωστόσο, αποτυγχάνει για τους ίδιους δομικούς λόγους με τον κεντρικό σχεδιασμό: ασυμμετρία πληροφόρησης, ελλείποντες βρόχοι ανάδρασης και αποσύνδεση των υπευθύνων λήψης αποφάσεων από τις συνέπειες των αποφάσεών τους.

Η παραδοχή αποτυγχάνει, για παράδειγμα, όταν το κόστος της θεσμικής διαμεσολάβησης υπερβαίνει την αξία της διαφοράς. Ας θεωρήσουμε έναν ενοικιαστή που ανακαλύπτει ότι το ενοικιαζόμενο διαμέρισμά του δεν διαθέτει το νομικά απαιτούμενο πιστοποιητικό ηλεκτρικής ασφάλειας—μια συνθήκη που θέτει άμεσο κίνδυνο για τη ζωή. Το νομικό δικαίωμα του ενοικιαστή να αποχωρήσει από τη σύμβαση είναι σαφές. Ωστόσο, το κόστος επιβολής αυτού του δικαιώματος μέσω του δικαστικού συστήματος υπερβαίνει τη χρηματική αξία της εγγύησης και των οφειλόμενων αποζημιώσεων, ακόμη και συμπεριλαμβανομένης πιθανής νόμιμης αποζημίωσης [1]. Η ορθολογική αντίδραση είναι να απορροφήσει κανείς την απώλεια και να αποχωρήσει.

Αυτό δεν είναι μια παθολογική ακραία περίπτωση. Είναι η προεπιλεγμένη εμπειρία για μια σημαντική κατηγορία διαφορών στις οποίες η βλάβη είναι πραγματική αλλά το χρηματικό διακύβευμα πέφτει κάτω από το όριο πέρα από το οποίο η θεσμική επιβολή γίνεται οικονομικά ορθολογική. Το αποτέλεσμα είναι

ένα σύστημα που δομικά ευνοεί τους κακόβουλους δράστες: όσοι βλάπτουν άλλους σε ποσά κάτω από αυτό το όριο μπορούν να δρουν ατιμώρητοι, επειδή το κόστος αναζήτησης δικαιοσύνης βαρύνει το ζημιωμένο μέρος.

Το παραπάνω παράδειγμα προέρχεται από το νομικό περιβάλλον του συγγραφέα—το τσεχικό αστικό δίκαιο. Σε άλλες νομικές παραδόσεις—το κοινό δίκαιο που βασίζεται σε προηγούμενα, το εθιμικό δίκαιο, τα μικτά συστήματα—η δικαιοσύνη αποτυγχάνει με διαφορετικούς τρόπους και σε διαφορετικό βαθμό, ανάλογα με τις πολιτισμικές και διαδικαστικές ιδιαιτερότητες της δικαιοδοσίας. Οι αναγνώστες πιθανότατα θα αναγνωρίσουν αντίστοιχα παραδείγματα από το δικό τους πλαίσιο. Αυτό που είναι δομικά καθολικό είναι το μοτίβο: διαφορές των οποίων η αξία πέφτει κάτω από το όριο της οικονομικά ορθολογικής επιβολής καταλήγουν με την απώλεια να απορροφάται από το ζημιωμένο μέρος. Το RSN δεν υπόσχεται τέλεια δικαιοσύνη—απλώς μειώνει το δομικό πλεονέκτημα που απολαμβάνουν οι κακόβουλοι δράστες όταν η θεσμική επιβολή είναι αντιστοιχοοικονομική.

1.2 Γιατί οι Υπάρχουσες Λύσεις Υστερούν

Τα πλαίσια Αποκεντρωμένης Ταυτότητας (DID) [2] παρέχουν κρυπτογραφικούς μηχανισμούς για τη διαχείριση αυτοκυρίαρχης ταυτότητας, αλλά επικεντρώνονται κυρίως στην επαλήθευση ταυτότητας χωρίς να αντιμετωπίζουν το ευρύτερο ζήτημα της συμπεριφορικής φήμης.

Τα Soulbound Tokens (SBTs) [3] συλλαμβάνουν τη διαπίστωση ότι η φήμη είναι μη μεταβιβάσιμη, αλλά βασίζονται σε υποδομή blockchain με περιορισμούς κλιμάκωσης και δεν αντιμετωπίζουν τα οικονομικά κίνητρα που διέπουν την εισαγωγή πληροφοριών. Σχετικές έννοιες, όπως τα merit tokens (π.χ. Liberland), μοιράζονται παρόμοια φιλοσοφία αλλά παραμένουν δεσμευμένες σε συγκεκριμένα δικαιοδοτικά πλαίσια.

Οι Αποκεντρωμένοι Αυτόνομοι Οργανισμοί (DAOs) [4] υλοποιούν τη διακυβέρνηση μέσω έξυπνων συμβολαίων, αλλά αναπαράγουν πλουτοκρατικές δυναμικές όπου η επιρροή είναι ανάλογη του κεφαλαίου. Η τετραγωνική ψηφοφορία [5] μετριάξει εν μέρει αυτό, αλλά περιορίζει την πρακτική υιοθέτηση. Οι DAOs αντιμετωπίζουν επίσης το θεμελιώδες πρόβλημα του *μαντείου (oracle problem)*: τα έξυπνα συμβόλαια δεν μπορούν να επαληθεύσουν αξιόπιστα καταστάσεις του πραγματικού κόσμου χωρίς μια αξιόπιστη εξωτερική πηγή, και αυτό το πρόβλημα δεν έχει γενική λύση

εντός της αρχιτεκτονικής blockchain.

Κανένα υπάρχον σύστημα δεν συνδυάζει αποκέντρωση, ανθεκτικότητα στη λογοκρισία, ψευδωνυμία, επαληθεύσιμο κόστος εισόδου και αναδύομενη συναίνεση.

1.3 Συνεισφορές

Η παρούσα εργασία προσφέρει τις ακόλουθες συνεισφορές:

1. Ορισμό του **Κοινωνικού Δικτύου Φήμης (RSN)**, ενός αποκεντρωμένου πρωτοκόλλου που επεκτείνει το πλαίσιο DID για να υποστηρίξει διμερή ανταλλαγή φήμης.
2. Ένα **μη ντετερμινιστικό πρωτόκολλο επιλογής επαληθευτή** βασισμένο σε συνεπή κατακερματισμό [6].
3. Την **Αρχή του Ακριβούς Ριζοσπαστισμού**, που τιμολογεί τους ισχυρισμούς ανάλογα με την απόστασή τους από τη συναίνεση του δικτύου μέσω τριών σωρευτικών καναλιών κόστους.
4. Ένα μοντέλο **Αξιόπιστης Αρχής** με ασύμμετρα κίνητρα, όπου η ψευδής έγκριση κοστίζει καταστροφικά περισσότερο από τα νόμιμα τέλη.
5. Μια **σταδιακή διαδρομή μετάβασης** μέσω παράλληλης δημοσιονομικής υποδομής.

2 Αρχές Σχεδιασμού

Η αρχιτεκτονική του RSN περιορίζεται από πέντε μη διαπραγματεύσιμες αρχές σχεδιασμού.

Συνέχεια και Εξέλιξη. Το σύστημα συνυπάρχει με τους υπάρχοντες θεσμούς κατά τη διάρκεια μιας μεταβατικής περιόδου απροσδιόριστης διάρκειας. Η μετάβαση πρέπει να είναι αναστρέψιμη σε κάθε στάδιο.

Εθελοντικότητα και Ευθύνη. Η συμμετοχή είναι εθελοντική, αλλά η εθελοντικότητα συνδέεται με την ευθύνη: ένας συμμετέχων που αναλαμβάνει τον έλεγχο μιας θεσμικής λειτουργίας ταυτόχρονα αναλαμβάνει και τις συνοδευτικές υποχρεώσεις.

Πολυμορφία και Πολιτισμική Ουδετερότητα. Η συναίνεση αναδύεται από διμερείς αλληλεπιδράσεις, όχι από προκαθορισμένους κανόνες που επιβάλλονται από τους σχεδιαστές του συστήματος.

Ανθεκτικότητα και Αντίσταση στη Λογοκρισία. Το κόστος λογοκρισίας του δικτύου πρέπει να υπερβαίνει το κόστος ανοχής του. Μόνο ο πλήρης ολοκληρωτισμός—με καταστροφικό πολιτικό και οικονομικό κόστος—μπορεί να καταστείλει το σύστημα.

Συναίνεση και Επιβολή. Το σύστημα ενσωματώνει τις ανθρώπινες τάσεις προς τη μικροπρέπεια, την κακία και την τιμωρητική ικανοποίηση ως φέροντα χαρακτηριστικά. Η κακή συμπεριφορά δεν απαγορεύεται· τιμολογείται.

3 Επισκόπηση Συστήματος

3.1 Κοινωνικό Δίκτυο Φήμης

Το RSN είναι ένα αποκεντρωμένο, ομότιμο (peer-to-peer) επίπεδο επικοινωνίας στο οποίο οι συμμετέχοντες ανταλλάσσουν επαληθεύσιμες πληροφορίες σχετικά με τη συμπεριφορά στον πραγματικό κόσμο. Οι καθοριστικές ιδιότητές του είναι: αποκεντρωμένη και μη λογοκρίσιμη υποδομή· ψευδώνυμη συμμετοχή μέσω DIDs· ασύμμετρη δομή κόστους (η ανάγνωση είναι φθηνή, η εγγραφή είναι ακριβή)· κρυπτογραφική επαληθευσσιμότητα· και **υποστήριξη προτύπων**—μηχανικά αναγνώσιμες μορφές για τις πληροφορίες που διαδίδονται μέσω του δικτύου, για τις υπηρεσίες που προσφέρουν οι αρχές (σύνθεση ισχυρισμού, έγκριση, υπηρεσία μάρτυρα), και για τη μορφή της πολιτικής συμπεριλαμβανομένων των κανόνων για την αξιολόγηση της φήμης του αντισυμβαλλομένου και την εκτίμηση του κινδύνου αναντιστοιχίας πολιτικής (μεταξύ δηλωμένης και πραγματικής συμπεριφοράς).

3.2 Αρχιτεκτονικά Στοιχεία

Το RSN αποτελείται από τέσσερα κύρια στοιχεία (Σχ. 1):

1. **Επίπεδο DID.** Ταυτότητες συμμετεχόντων με δηλωμένους κανόνες, μεταδεδομένα φήμης και δρομολόγηση δικτύου.
2. **Πρωτόκολλο Ισχυρισμών.** Δομημένη μορφή για τη δημοσίευση δηλώσεων σχετικά με γεγονότα του πραγματικού κόσμου.
3. **Δίκτυο Επαλήθευσης.** Αποκεντρωμένο πρωτόκολλο για την ανάθεση επαληθευτών με χρήση συνεπούς κατακερματισμού.
4. **Επίπεδο Συγκέντρωσης Φήμης.** Υπηρεσίες που παράγουν αναγνώσιμες από τον άνθρωπο συνόψεις φήμης.

3.3 Ρόλοι Συμμετεχόντων

Μια συναλλαγή επαλήθευσης εμπλέκει έως έξι διακριτούς ρόλους DID (Σχ. 2): **Εκδότης** (DID_I , δημιουργεί και υποβάλλει τον ισχυρισμό), **Υποκείμενο** (DID_S , το DID για το οποίο αφορά ο

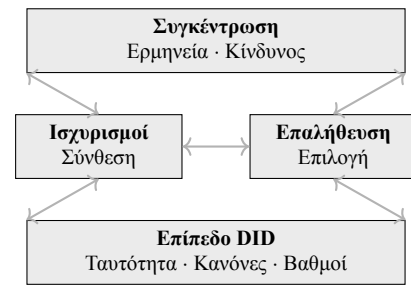


Figure 1: Αρχιτεκτονική τεσσάρων επιπέδων του RSN.

ισχυρισμός—μπορεί να συμπίπτει με τον Εκδότη), **Αρχή** (DID_A , εγκρίνει τον ισχυρισμό έναντι αμοιβής· μπορεί επίσης να προσφέρει υπηρεσίες μάρτυρα—*προαιρετικό*), **Μάρτυρας** ($DID_{W_{1..n}}$, ανώνυμος επόπτης της εντιμότητας του επαληθευτή μέσω κωδικών πρόκλησης—*προαιρετικό*), **Επαληθευτής** (DID_V , επιλεγμένος αλγοριθμικά για να δημοσιεύσει τον ισχυρισμό), και το **RSN** (το δίκτυο όπου δημοσιεύονται οι επαληθευμένοι ισχυρισμοί). Οποιοσδήποτε ρόλος μπορεί να ανατεθεί σε άλλο DID (Ενότητα 7.4). Μια Αρχή συνήθως συνδυάζει την έγκριση με υπηρεσίες μάρτυρα, αλλά οι δύο λειτουργίες είναι λογικά ανεξάρτητες.

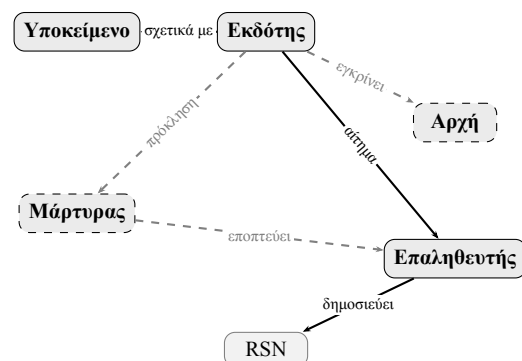


Figure 2: Ρόλοι DID σε μια συναλλαγή επαλήθευσης. Διακεκομμένο = προαιρετικό (Αρχή, Μάρτυρας).

3.4 Αδιαφθορία: Τέσσερις Δυνάμεις

Η αδιαφθορία του RSN δεν προκύπτει από έναν μόνο μηχανισμό, αλλά από τέσσερις ταυτόχρονες δυνάμεις. Καμία δεν επαρκεί από μόνη της· μόνο ο συνδυασμός τους καθιστά μια απόπειρα διαφθοράς οικονομικά παράλογη.

Απρόβλεπτος στόχος. Ο επαληθευτής για κάθε ισχυρισμό επιλέγεται μη ντετερμινιστικά μέσω συνεπούς κατακερματισμού (Ενότητα 5.3). Ένας επιτιθέμενος δεν μπορεί να στοχεύσει εκ των προτέρων έναν συγκεκριμένο επαληθευτή για δωροδοκία, επειδή η ταυτότητα του επαληθευτή είναι

συνάρτηση του περιεχομένου του ισχυρισμού και των προηγούμενων επαναλήψεων, όχι της επιλογής του εκδότη.

Μόχλευση φήμης—αργή άνοδος, γρήγορη πτώση. Η φήμη μπορεί να κερδηθεί μόνο σταδιακά, μέσω διαρκούς συνεπούς συμπεριφοράς. Μπορεί όμως να χαθεί καταστροφικά με μία μόνο δόλια έγκριση (Ενότητα 6.2). Αυτή η ασυμμετρία σημαίνει ότι χρόνια συσσωρευμένης φήμης μπορούν να καταστραφούν από μία ανέντιμη έγκριση· η βέλτιστη στρατηγική παραμένει η απόρριψη ύποπτων ισχυρισμών.

Δημόσια υπόσχεση. Κάθε Κάτοχος DID δηλώνει δημόσια την πολιτική του—ένα μηχανικά αναγνώσιμο σύνολο κανόνων που δεσμεύεται να ακολουθεί. Η απόκλιση μεταξύ της δήλωσης και της πραγματικής συμπεριφοράς είναι ανιχνεύσιμη και τιμολογείται ως παράπτωμα φήμης βαρύτερο από την υποκείμενη παραβίαση (Ενότητα 7.3). Η υποκρισία είναι επομένως πιο δαπανηρή από την άμεση ανεντιμότητα.

Ασυμμετρία κόστους επίθεσης πλέγματος. Το κόστος λογοκρισίας ή αποσταθεροποίησης του δικτύου αυξάνεται μη γραμμικά με το μέγεθος και την πυκνότητα του δικτύου, ενώ το κόστος ανοχής του παραμένει σταθερό. Για να αποδώσει η λογοκρισία, ένας κεντρικοποιημένος δρόντας θα έπρεπε να την εφαρμόσει σε ολόκληρο το δίκτυο—απαιτώντας μέτρα δυσανάλογα προς οποιοδήποτε νοητό όφελος (Ενότητα 10).

4 Μοντέλο Αποκεντρωμένης Ταυτότητας

4.1 DID με Ειδικές Ιδιότητες

Το RSN επεκτείνει την προδιαγραφή W3C DID Core [2] με: **Δηλωμένους Κανόνες** (μηχανικά αναγνώσιμες συμπεριφορικές δεσμεύσεις), **Μεταδεδομένα Φήμης** (συγκεντρωτικός βαθμός συμπεριφοράς), και **Δρομολόγηση Δικτύου** (μεταβλητή πύλη onion, ξεχωριστή από τη σταθερή θέση στον δακτύλιο).

4.2 Κύκλος Ζωής Ισχυρισμού

Ένας Ισχυρισμός διέρχεται από έξι στάδια (Σχ. 3): σύνθεση, προαιρετική έγκριση από αρχή, επιλογή επαληθευτή μέσω συνεπούς κατακερματισμού, απόφαση επαλήθευσης (αποδοχή ή απόρριψη με επανάληψη), δημοσίευση, και ενημέρωση φήμης για όλα τα μέρη.

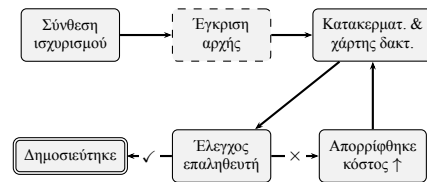


Figure 3: Κύκλος ζωής ισχυρισμού με βρόχο επανάληψης.

4.3 Σχέση με το W3C DID Core

Το μοντέλο ταυτότητας του RSN αποτελεί γνήσιο υπερσύνολο της προδιαγραφής W3C DID Core [2]. Όλα τα DIDs του RSN είναι έγκυρα W3C DIDs. Οι ειδικές επεκτάσεις του RSN κωδικοποιούνται ως ιδιότητες εγγράφου DID που ορίζονται σε μια αποκλειστική προδιαγραφή μεθόδου DID, συμβατή με υπάρχουσα υποδομή όπως το ION [7] και το Ceramic [8].

5 Επαλήθευση και Διάδοση Πληροφοριών

5.1 Κόστος Εισαγωγής Πληροφορίας

Η βασική οικονομική αρχή του RSN είναι η ασυμμετρία μεταξύ ανάγνωσης και εγγραφής. Η ανάγνωση δεδομένων φήμης προσεγγίζει το μηδενικό οριακό κόστος για τους συμμετέχοντες που αποτελούν μέρος του δικτύου DID και έχουν πρόσβαση ανάλογη της φήμης τους—οι νεοεισερχόμενοι πρέπει να κερδίσουν σταδιακά ευρύτερη πρόσβαση (βλ. αντι-παρασιτισμό). Η εγγραφή—νοούμενη ως η ανθεκτική υλοποίηση της φήμης στο δίκτυο, όχι ως μια εφάπαξ τεχνική πράξη—απαιτεί επαληθεύσιμη σωρευτική επένδυση σε τρεις διαστάσεις: **χρόνο** (χρόνια ζωής αφιερωμένα σε συνεπή συμπεριφορά, εκπληρωμένες δεσμεύσεις και καλλιεργημένες σχέσεις), **ενέργεια** (προσπάθεια επενδυμένη σε έντιμες συναλλαγές, φροντίδα για τις συνεργασίες και μακροπρόθεσμη αξιοπιστία), και **χρήμα** (επένδυση στο ίδιο το όνομά του—επαγγελματική ανάπτυξη, ποιότητα της εργασίας του, αποκατάσταση για προκληθείσες βλάβες). Η φήμη δεν μπορεί να αγοραστεί ακαριαία—είναι το αποτέλεσμα ισόβιας συσσώρευσης που το σύστημα απλώς καθιστά ορατό και μεταβιβάσιμο μεταξύ πλαισίων. Το εφάπαξ τεχνικό κόστος του πρωτοκόλλου (κρυπτογραφικές υπογραφές, τέλη επαληθευτή) είναι αμελητέο σε σύγκριση με αυτήν την υποκείμενη επένδυση.

5.2 Κοινωνικός Γράφος και Βάθος Επαφών

Το RSN είναι θεμελιωδώς ένα κοινωνικό δίκτυο: κάθε DID προσθέτει επαφές (άλλα DIDs) που επιτρέπουν τη σύνδεση. Αυτές οι επαφές έχουν τις δικές τους επαφές, και ούτω καθεξής. Η αλγοριθμική αναζήτηση επαληθευτή λειτουργεί εντός ενός ρυθμιζόμενου βάθους h συνδεδεμένων επαφών (π.χ. $h = 3$: οι άμεσες επαφές κάποιου, οι επαφές τους, και οι επαφές των επαφών). Αυτή η αρχιτεκτονική δεν απαιτεί ένα ενιαίο παγκόσμιο blockchain—ευνοεί φυσικά την ανάδυση κοινοτήτων/συστάδων με επικαλύψεις σε άλλες κοινότητες. Κάθε συμμετέχων DID πρέπει να έχει μια δημοσιευμένη **πολιτική**—ένα μηχανικά αναγνώσιμο σύνολο κανόνων που διέπουν το πώς αξιολογούνται τα εισερχόμενα αιτήματα. Οι παραβιάσεις πολιτικής καταγράφονται στο δίκτυο ως αρνητικά τεχνουργήματα.

5.3 Αλγοριθμική Επιλογή Επαληθευτή

Το πρωτόκολλο επαλήθευσης χρησιμοποιεί συνεπή κατακερματισμό [6] (Σχ. 4). Η επαλήθευση είναι μια αμειβόμενη υπηρεσία: οι επαληθευτές λειτουργούν έναντι αμοιβής, δημιουργώντας μια αγορά όπου ο ανταγωνισμός καθορίζει την τιμολόγηση, την ταχύτητα και την αξιοπιστία.

Βήμα 1. Το έγγραφο του ισχυρισμού συνενώνεται με το αποτέλεσμα κατακερματισμού της προηγούμενης επανάληψης (ή $\emptyset$ στην πρώτη επανάληψη) και κατακερματίζεται:

$$\text{pos} = f_h(\text{claim} \parallel \text{prev_hash}) \quad (1)$$

Ο αλγόριθμος πρέπει να περιλαμβάνει την *πλήρη διαδρομή* όλων των προηγούμενων αιτημάτων και απαντήσεων—όχι απλώς έναν κατακερματισμό της προηγούμενης επανάληψης. Η πλήρης απάντηση κάθε επαληθευτή (αποδοχή, απόρριψη, τιμή προσφοράς, αιτιολογία) προσαρτάται στο αυξανόμενο έγγραφο, επαληθεύσιμη μέσω κρυπτογραφικών υπογραφών σε κάθε βήμα.

Βήμα 2. Ο κατακερματισμός αντιστοιχίζεται σε N θέσεις στον δακτύλιο συνεπούς κατακερματισμού, ομοιόμορφα κατανεμημένες (π.χ. για $N = 4$: $+0^\circ, +90^\circ, +180^\circ, +270^\circ$). Από κάθε θέση, μια δεξιόστροφη αναζήτηση επιλέγει το πλησιέστερο DID ως υποψήφιο επαληθευτή (Σχ. 5). Το N είναι μια μεταβλητή παράμετρος που μπορεί να εξαρτάται από το ποσοστό των τρέχοντων ενεργών DIDs, την ώρα της ημέρας ή την ιστορική ανταπόκριση του δικτύου.

Βήμα 3. Ο Επαληθευτής αποδέχεται (δημοσιεύει, διακινδυνεύοντας φήμη) ή απορρίπτει (επιστρέφοντας

στο Βήμα 1 με τον κατακερματισμό απόρριψης). Όταν ένας κόμβος δεν ανταποκρίνεται παρά τη δηλωμένη κατάσταση διαδικτυακής παρουσίας, το επόμενο αίτημα πρέπει να περιλαμβάνει όλες τις απαντήσεις από όλους τους N προηγούμενους υποψήφιους επαληθευτές.

Αντι-παρασιτισμός. Τα στοχευμένα DIDs μπορούν να ορίσουν τέλη ή περιορισμούς πρόσβασης για ερωτήματα από νέα DIDs με μικρή φήμη. Αυτός ο διαβαθμισμένος μηχανισμός (όχι δυαδικός) αναγκάζει τους νεοεισερχόμενους να χτίσουν φήμη μέσω γνώσιας δραστηριότητας πριν καταναλώσουν ελεύθερα τα δεδομένα άλλων.

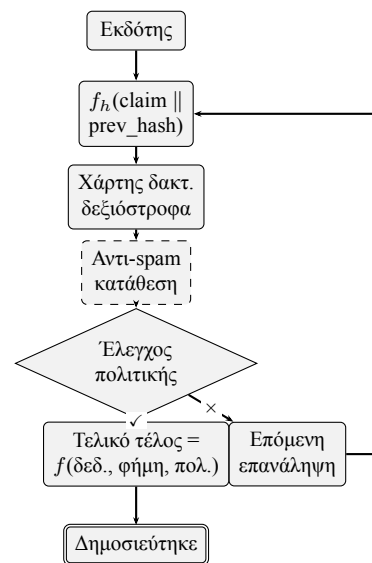


Figure 4: Πρωτόκολλο επιλογής επαληθευτή. Η αντι-spam κατάθεση είναι προαιρετική και μπορεί να επιστρέφεται. Το τελικό τέλος καταβάλλεται μόνο κατά την αποδοχή.

Κάθε απόρριψη προσαρτά την πλήρη απάντηση του επαληθευτή (συμπεριλαμβανομένων των λόγων και των προϋποθέσεων) στο έγγραφο του ισχυρισμού, διευρύνοντας το περιεχόμενό του. Από το διευρυμένο έγγραφο, υπολογίζεται μη ντετερμινιστικά ένας νέος κατακερματισμός, που αντιστοιχίζεται σε διαφορετική θέση στον δακτύλιο και επιλέγει διαφορετικό επαληθευτή. Η τεκμηρίωση της πλήρους διαδρομής είναι υποχρεωτική—ο εκδότης δεν μπορεί να προβλέψει ή να επηρεάσει τον επόμενο επαληθευτή. Αν ένας επαληθευτής αγνοήσει ένα αίτημα παρά τη συμβατή δηλωμένη πολιτική, οι μάρτυρες (αν υπάρχουν) το καταγράφουν, και ο εκδότης μπορεί να επισυνάψει αποδεικτικά στοιχεία μάρτυρα κατά την τελική δημοσίευση.

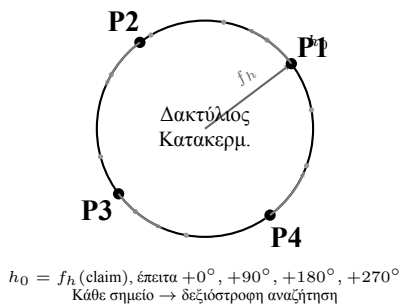


Figure 5: Επιλογή πολλαπλών σημείων ($N=4$). Ο κατακερματισμός h_0 ορίζει τη μετατόπιση· 4 σημεία ομοιόμορφα κατανεμημένα από το h_0 .

5.4 Πρωτόκολλο Μάρτυρα

Ο ρόλος του **Μάρτυρα** παρέχει ανώνυμη λογοδοσία για την εντιμότητα του επαληθευτή μέσω ενός κρυπτογραφικού πρωτοκόλλου κωδικών πρόκλησης:

Βήμα W1. Ο αιτών υπογράφει το αίτημα επαλήθευσης και το στέλνει σε N_w μάρτυρες—επαφές από το κοινωνικό δίκτυο του αιτούντος, ή εξειδικευμένους παρόχους υπηρεσιών μάρτυρα που λειτουργούν έναντι αμοιβής.

Βήμα W2. Κάθε μάρτυρας w_i υπογράφει ολόκληρο το υπογεγραμμένο αίτημα, διατηρεί την αρχική υπογραφή σ_i , και υπολογίζει έναν κωδικό πρόκλησης $c_i = h(\sigma_i)$. Ο κωδικός πρόκλησης προσαρτάται στο αίτημα.

Βήμα W3. Το αίτημα, φέροντας πλέον N_w κωδικούς πρόκλησης, στέλνεται στον επαληθευτή. Ο επαληθευτής παρατηρεί τους κωδικούς αλλά *δεν μπορεί να προσδιορίσει* ποιοι είναι οι μάρτυρες ή αν οι κωδικοί αντιστοιχούν σε πραγματικές υπογραφές.

Βήμα W4 (έντιμος επαληθευτής). Αν ο επαληθευτής ανταποκριθεί σύμφωνα με τη δηλωμένη πολιτική του, οι κωδικοί πρόκλησης παραμένουν αδιαφανείς. Οι μάρτυρες δεν αποκαλύπτονται ποτέ. Δεν δημοσιεύονται πρόσθετα δεδομένα.

Βήμα W5 (παραβίαση πολιτικής). Αν ο επαληθευτής παραβιάσει την πολιτική του (αγνοήσει το αίτημα, ανταποκριθεί ασυνεπώς), ο αιτών κατέχει τις αρχικές υπογραφές των μαρτύρων σ_i . Αυτές μπορούν να δημοσιευτούν ως συνοδευτικά δεδομένα: οποιοσδήποτε μπορεί να επαληθεύσει ότι $c_i = h(\sigma_i)$, αποδεικνύοντας ότι ο μάρτυρας ήταν παρών. Ο αιτών μπορεί να δημοσιεύσει ανεξάρτητα—ο επαληθευτής έχει ήδη υπογράψει τους κωδικούς πρόκλησης στην απάντησή του.

Η ιδιότητα της μπλόφας. Ο αιτών μπορεί να αντικαταστήσει τυχαίες τιμές για ορισμένους ή όλους τους κωδικούς πρόκλησης. Ο επαληθευτής

δεν μπορεί να διακρίνει τους γνήσιους κωδικούς (υποστηριζόμενους από αρχές υψηλής φήμης) από τον θόρυβο. Αυτή η *αβεβαιότητα* είναι ο μηχανισμός επιβολής: κάθε αίτημα φέρει τον κίνδυνο ότι μια σεβαστή αρχή παρακολουθεί ανώνυμα. Το κόστος διατήρησης αυτής της πίεσης είναι σχεδόν μηδενικό (παραγωγή τυχαίων αριθμών), ενώ το πιθανό κόστος της ανεντιμότητας για τον επαληθευτή είναι καταστροφικό. Η έντιμη συμπεριφορά ενθαρρύνεται ακόμη και απουσία πραγματικών μαρτύρων.

Η Αρχή ως μάρτυρας. Μια Αρχή που εγκρίνει έναν ισχυρισμό μπορεί να συνδυάσει υπηρεσίες μάρτυρα: “Εγκρίνω τον ισχυρισμό σου και υπηρετώ ως ανώνυμος μάρτυρας κατά την επαλήθευση.” Αυτό είναι ένα φυσικό επιχειρηματικό μοντέλο—η Αρχή έχει ήδη το πλαίσιο. Ωστόσο, οι δύο ρόλοι είναι λογικά ανεξάρτητοι.

5.5 Η Αρχή του Ακριβούς Ριζοσπαστισμού

Τρία κανάλια κόστους σωρεύονται ταυτόχρονα (Σχ. 6):

Κανάλι 1: Κόστος Επανάληψης. Κάθε απόρριψη επιβάλλει μια νέα επανάληψη που καταναλώνει χρόνο και πόρους. Γραμμική αύξηση.

Κανάλι 2: Διόγκωση Εγγράφου. Κάθε επανάληψη προσθέτει την πλήρη απάντηση του επαληθευτή στο έγγραφο του ισχυρισμού. Η αύξηση είναι γραμμική, αλλά με μια βασική μετατόπιση: το αρχικό ωφέλιμο φορτίο (περιεχόμενο ισχυρισμού, έγκριση αρχής, κρυπτογραφικές υπογραφές) έχει ήδη μη τετριμμένο μέγεθος B_0 . Συνολικό μέγεθος μετά από k επαναλήψεις: $S(k) = B_0 + k \cdot \Delta$, όπου Δ είναι το μέσο μέγεθος απάντησης.

Κανάλι 3: Ασφάλιστρο Κινδύνου Επαληθευτή. Ο κίνδυνος είναι υποκειμενικός. Ο επαληθευτής αξιολογεί κατά πόσο οι δηλωμένες πολιτικές του αιτούντος DID συγκρούονται με τα δικά του εμπορικά, κοινωνικά ή πολιτικά συμφέροντα. Το ασφάλιστρο μπορεί να κλιμακωθεί εκθετικά με την αντιλαμβανόμενη απόσταση από το “ιδανικό” του επαληθευτή: $P(d) = \alpha \cdot e^{\beta d}$, όπου d είναι η υποκειμενική μετρική απόστασης του επαληθευτή. Πέρα από ένα προσωπικό όριο απαγόρευσης, ο επαληθευτής μπορεί να αρνηθεί εντελώς.

Κρίσιμα, αυτό δεν είναι λογοκρισία. Κανένας ισχυρισμός δεν απαγορεύεται. Το σύστημα τιμολογεί τον κίνδυνο (Πίν. 1).

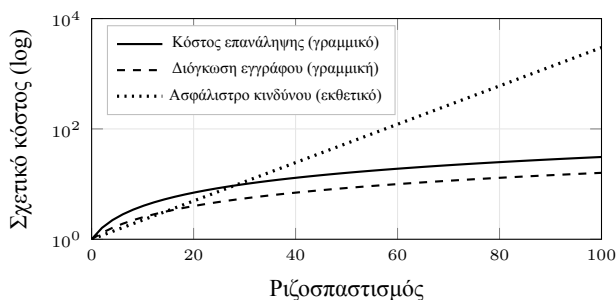


Figure 6: Κλιμάκωση κόστους στα τρία κανάλια. Το ασφάλιστρο κινδύνου κυριαρχεί σε υψηλό ριζοσπαστισμό.

Table 1: Σύγκριση κόστους ανά τύπο ισχυρισμού.

Τύπος	Επαν.	Έγγρ.	Τέλος	Σύνολο
Αξιοπίστος	$k_{\min}$	B_0	$P_{\min}$	Χαμηλό
Αμφιλεγόμενος	k_{med}	$B_0 + k\Delta$	$\alpha e^{\beta d}$	Μέτριο
Ριζοσπαστικός	$k_{\max}$	$\gg B_0$	$\gg P_{\min}$	Πολύ υψηλό
Δόλιος	$\rightarrow \infty$	—	—	Αδημοσίευτος

6 Φήμη και Εκτίμηση Κινδύνου

6.1 Μοντέλο Συσσώρευσης Φήμης

Η φήμη παρουσιάζει τρεις ιδιότητες: **αργή συσσώρευση** (σταδιακή αύξηση μέσω συνεπούς συμπεριφοράς), **ταχεία καταστροφή** (μία μόνο απάτη μπορεί να μειώσει καταστροφικά τον βαθμό), και **ατομική αξιολόγηση** (κάθε καταναλώνων μέρος μπορεί να εφαρμόσει τη δική του συνάρτηση συγκέντρωσης).

6.2 Αξιοπίστες Αρχές

Μια Αξιοπίστη Αρχή εξετάζει τους ισχυρισμούς και, αν ικανοποιηθεί, τους συνυπογράφει—διακινδυνεύοντας τη δική της φήμη (Σχ. 7). Η ασυμμετρία είναι σκόπιμη: η απόκτηση φήμης είναι αργή (σταδιακό $+\delta$ ανά έντιμη έγκριση), ενώ η απώλειά της είναι καταστροφική ($-\Delta \gg \delta$ ανά ψευδή έγκριση· ενδεικτικά, π.χ. $+2\%$ έναντι -70%). Η βέλτιστη στρατηγική είναι πάντα η απόρριψη ύποπτων ισχυρισμών. Οι συγκεκριμένες τιμές των δ και Δ είναι παράμετροι του συστήματος.

6.3 Πολυδιάστατη Φήμη

Η φήμη δεν είναι ένα βαθμωτό μέγεθος αλλά ένα διάνυσμα σε πολλαπλές διαστάσεις: χρηματοοικονομική αξιοπιστία, προσωπική ακεραιότητα, επαγγελματική επάρκεια, πολιτειακή δέσμευση και άλλες (Σχ. 8). Διαφορετικοί πάροχοι

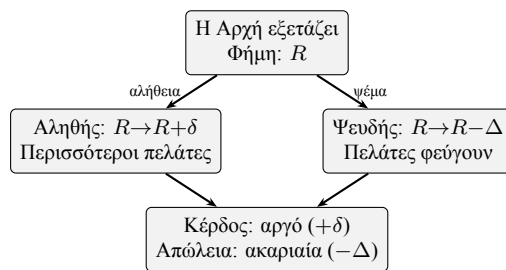


Figure 7: Αξιοπίστη Αρχή—ασύμμετρα κίνητρα.

αξιολόγησης προβάλλουν αυτό το διάνυσμα διαφορετικά ανάλογα με το πλαίσιο—ένας δανειστής δίνει προτεραιότητα στη χρηματοοικονομική αξιοπιστία, ένας εργοδότης στην επαγγελματική επάρκεια, ένας γείτονας στην πολιτειακή συμπεριφορά. Δεν υπάρχει ένας μοναδικός “σωστός” βαθμός φήμης· μόνο οπτικές γωνίες.

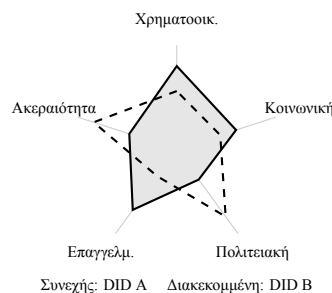


Figure 8: Πολυδιάστατα διανύσματα φήμης. Διαφορετικά DIDs παρουσιάζουν διαφορετικά προφίλ στις διαστάσεις.

6.4 Εκδημοκρατισμένη Εκτίμηση Κινδύνου

Το RSN εκδημοκρατίζει τη συστηματική εκτίμηση κινδύνου—μία δυνατότητα που σήμερα συγκεντρώνεται στα χρηματοπιστωτικά ιδρύματα αλλά είναι εφαρμόσιμη πολύ πέρα από τον τραπεζικό τομέα. Βιομηχανικοί όμιλοι που αξιολογούν την αξιοπιστία προμηθευτών, ασφαλιστικές εταιρείες που τιμολογούν συμπεριφορικό κίνδυνο, δέουσα επιμέλεια για συγχωνεύσεις και εξαγορές, εκτίμηση διάρκειας ζωής εξοπλισμού στη μεταποίηση—οπουδήποτε ο κίνδυνος αντισυμβαλλομένου απαιτεί αξιολόγηση, το RSN παρέχει μια αποκεντρωμένη, καθοδηγούμενη από την αγορά εναλλακτική. Μια αγορά υπηρεσιών ερμηνείας μεταφράζει τα ακατέργαστα πολυδιάστατα δεδομένα φήμης σε αξιοποιήσιμες συνόψεις, καθιστώντας την αξιολόγηση αντισυμβαλλομένου προσβάσιμη σε κάθε συμμετέχοντα με οριακό κόστος.

7 Συναίνεση και Επίλυση Διαφορών

7.1 Μοντέλο Αποκεντρωμένης Δικαιοσύνης

Το RSN αναπλαισιώνει τη δικαιοσύνη ως πρόβλημα διμερούς διαπραγμάτευσης. Η απειλή μόνιμης, επαληθεύσιμης ζημίας στη φήμη είναι πιο αποτελεσματικός αποτρεπτικός παράγοντας από νομικές διαδικασίες που το ζημιωμένο μέρος δεν μπορεί να αντέξει οικονομικά.

7.2 Αναδυόμενη Συναίνεση

Κάθε συμμετέχων διατηρεί ένα προσωπικό όριο ικανοποίησης. Η συνολική συναίνεση του δικτύου αναδύεται ως ο στατιστικός μέσος όρος χιλιάδων διμερών διαπραγματεύσεων (Σχ. 9). Μια αντίδραση πολύ πάνω από τη συναίνεση (βάρβαρη) είναι ακριβή στη δημοσίευση. Μια αντίδραση κοντά στη συναίνεση (αναλογική) είναι φθηνή. Η συναίνεση δεν είναι κανόνας—είναι ένα σήμα τιμής.

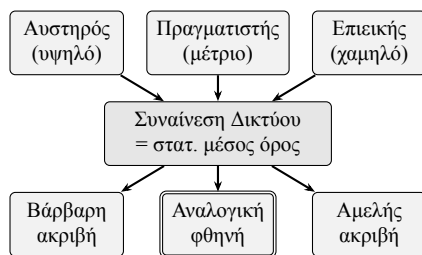


Figure 9: Αναδυόμενη συναίνεση από ατομικά όρια ικανοποίησης.

7.3 Βαθμονόμηση Τιμωρίας

Κάθε Κάτοχος DID δηλώνει δημόσια τις αντιδράσεις σε συγκεκριμένες κατηγορίες παραπτωμάτων. Δυσανάλογα αυστηρές ή επιεικές δηλώσεις προσελκύουν αρνητικά σήματα φήμης. Οι αναλογικές δηλώσεις γίνονται αποδεκτές χωρίς τριβή—ένα αυτο-βαθμονομούμενο σύστημα τιμωρίας.

Οι δηλώσεις συναίνεσης υπόκεινται και οι ίδιες σε ανίχνευση υποκρισίας: η δηλωτική δέσμευση σε μια θέση συναίνεσης ενώ κανείς συμπεριφέρεται ασυνεπώς συνιστά παράπτωμα φήμης βαρύτερο από την υποκείμενη απόκλιση, καθώς αποδεικνύει σκόπιμη εξαπάτηση.

7.4 Ανάθεση

Όλες οι δραστηριότητες εντός ενός DID—με μία εξαίρεση—μπορούν να ανατεθούν σε άλλο DID. **Ο ρόλος του Υποκειμένου—το DID για τη**

συμπεριφορά του οποίου αφορά ο ισχυρισμός—δεν μπορεί να ανατεθεί· είναι αμετάκλητα δεσμευμένος στον κάτοχο ταυτότητας στον οποίο αναφέρεται ο ισχυρισμός. Οι υπόλοιποι ενεργοί ρόλοι—Εκδότης, Αρχή, Μάρτυρας, Επαληθευτής—μπορούν να μεταβιβαστούν σε ένα ορισμένο εξουσιοδοτημένο DID, είτε για επαλήθευση, υποβολή ισχυρισμού, συμμετοχή σε συναίνεση, ή επίλυση διαφορών. Η ανάθεση είναι ανακλητή ανά πάσα στιγμή. Αυτό επιτρέπει την εξειδίκευση (π.χ. επαγγελματικές υπηρεσίες επαλήθευσης) ενώ ο Κάτοχος διατηρεί τον απόλυτο έλεγχο και την ευθύνη. Η ανάθεση εφαρμόζεται σε ολόκληρο το σύστημα και είναι ουσιώδης για την κλιμάκωση.

7.5 Από την Ατομική Ηθική στο Αναδυόμενο Κοινωνικό Συμβόλαιο

Η δηλωμένη πολιτική κάθε DID αντιπροσωπεύει μια τυποποίηση της ατομικής ηθικής: τι θεωρεί αποδεκτό ο Κάτοχος, πώς αντιδρά σε συγκεκριμένες συμπεριφορές, τι απαιτεί από τους αντισυμβαλλομένους. Αυτές οι πολιτικές δεν επιβάλλονται από έναν σχεδιαστή συστήματος—επιλέγονται από κάθε συμμετέχοντα και εκφράζονται σε μηχανικά αναγνώσιμη μορφή.

Αυτή η τυποποίηση επιτρέπει μια τριβάθμια ανάπτυξη. Πρώτον, η ατομική ηθική κωδικοποιείται ως **πολιτική**—ένα σύνολο δηλωμένων κανόνων, ορίων και συναρτήσεων απόκρισης που το DID δεσμεύεται να ακολουθεί. Δεύτερον, το σύνολο όλων των πολιτικών σε όλο το δίκτυο παράγει **αναδυόμενη ηθική**—στατιστικά παρατηρήσιμες νόρμες που κανένας μεμονωμένος συμμετέχων δεν σχεδίασε αλλά που προκύπτουν από την αλληλεπίδραση χιλιάδων ατομικών ηθικών θέσεων [9]. Τρίτον, αυτή η αναδυόμενη ηθική, εκφρασμένη ως κοινές συμπεριφορικές νόρμες που επιβάλλονται μέσω διμερών σημάτων τιμής, συνιστά ένα **μετρήσιμο κοινωνικό συμβόλαιο**—όχι ένα θεωρητικό κατασκεύασμα που κανείς δεν υπέγραψε [10], αλλά ένα εμπειρικά παρατηρήσιμο σύνολο κανόνων που υποστηρίζεται από πραγματική συμπεριφορά.

Αυτή η διαδικασία αντικατοπτρίζει ευρήματα από τη θεωρία των ηθικών θεμελίων [11]: η ανθρώπινη ηθική είναι διαισθητική, πλουραλιστική και πολιτισμικά μεταβλητή. Το RSN δεν απαιτεί ηθική συναίνεση ως είσοδο· παράγει συμπεριφορική συναίνεση ως έξοδο. Το προκύπτον κοινωνικό συμβόλαιο δεν είναι στατικό—εξελίσσεται καθώς οι συμμετέχοντες εντάσσονται, αποχωρούν και προσαρμόζουν τις πολιτικές τους ως αντίδραση στην ανάδραση του δικτύου. Σε αντίθεση με την

κλασική θεωρία του κοινωνικού συμβολαίου, αυτό το συμβόλαιο είναι ανακλητό, παρατηρήσιμο και επιβλητό χωρίς κυρίαρχο.

8 Οικονομικό Μοντέλο

Οι προηγούμενες ενότητες περιέγραψαν ένα εργαλείο—τους μηχανισμούς επαλήθευσης, τη δομή κόστους και την αναδυόμενη συναίνεση του RSN. Η παρούσα ενότητα περιγράφει μια μεθοδολογία για την εφαρμογή αυτού του εργαλείου στη δημοσιονομική μετάβαση και τη μετάβαση διακυβέρνησης. Το εργαλείο είναι γενικής χρήσης· η παρακάτω μεθοδολογία είναι μία πιθανή εφαρμογή.

8.1 Δομή Κινήτρων

Η φήμη ως κεφάλαιο δημιουργεί άμεσα κίνητρα για έντιμη συμπεριφορά. Στην κανονική λειτουργία, οι συμμετέχοντες χτίζουν φήμη φυσικά μέσω καθημερινών συναλλαγών και εκπληρωμένων δεσμεύσεων. Η κύρια δαπάνη αφορά τους *αρνητικούς* ισχυρισμούς—την καταγραφή βλάβης που προκάλεσαν άλλοι. Αυτή η ασυμμετρία δίνει κίνητρο για χρήσιμη, αξιόπιστη συμπεριφορά: το να είσαι έντιμος δεν κοστίζει τίποτα επιπλέον, ενώ το να είσαι επιβλαβής δημιουργεί ένα τεκμηριωμένο ίχνος που άλλοι θα πληρώσουν για να διατηρήσουν. Η υποκρισία—η δήλωση κανόνων χωρίς την τήρησή τους—είναι ο πιο δαπανηρός τρόπος αποτυχίας, καθώς αποδεικνύει σκόπιμη εξαπάτηση.

8.2 Παράλληλο Δημοσιονομικό Σύστημα

Τρία στοιχεία επιτρέπουν ανταγωνιστική πίεση: (1) **Απλός Φόρος**—ένας ενιαίος αναλογικός συντελεστής χωρίς εξαιρέσεις, αρχικά οριακά κάτω από τον υφιστάμενο πραγματικό συντελεστή· (2) **Ηλεκτρονική Καταχώριση Δαπανών (ESR)**—αντιστρέφοντας το τσεχικό μοντέλο EET ώστε οι πολίτες να επιτηρούν τις κρατικές δαπάνες· (3) **Κατανομή Φόρου Καθοδηγούμενη από τον Πολίτη**—ξεκινώντας από λίγα τοις εκατό τον πρώτο χρόνο και φτάνοντας, μετά από μια δεκαετία, οπουδήποτε από χαμηλά δινήφια ποσοστά έως πλήρη μετάβαση σε ένα σύστημα καθοδηγούμενο από τον πολίτη, ανάλογα με τον ρυθμό υιοθέτησης. Ο πραγματικός ρυθμός εξαρτάται από την ταχύτητα με την οποία αναδύονται εναλλακτικές ελεύθερης αγοράς στις κρατικές υπηρεσίες και από την προθυμία του κράτους να συνεργαστεί με τη μετάβαση· η συνάρτηση του χρόνου δεν χρειάζεται να είναι

γραμμική, και δεν υπάρχει λόγος να τεθεί ανώτατο όριο στο πού μπορεί τελικά να φτάσει η υιοθέτηση.

9 Διαδρομή Μετάβασης

Η μετάβαση προχωρά σε τρεις φάσεις (Σχ. 10): **Φάση 1: Επικάλυψη** (το RSN ως πληροφοριακό επίπεδο, το κράτος είναι ο μοναδικός πάροχος), **Φάση 2: Ανταγωνισμός** (το RSN παρέχει λειτουργικές εναλλακτικές, χρήση διπλού συστήματος), και **Φάση 3: Μετάβαση** (το RSN υπερτερεί των κρατικών ισοδυνάμων, εθελοντική μετανάστευση). Η μετάβαση είναι αναστρέψιμη σε κάθε στάδιο.

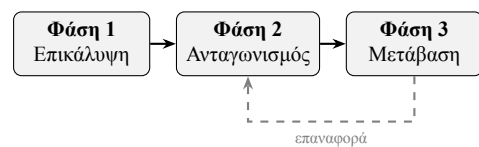


Figure 10: Τριφασική μετάβαση—αναστρέψιμη σε κάθε στάδιο.

Ο κύριος μηχανισμός πίεσης είναι δημοσιονομικός: όταν οι υπό όρους φορολογούμενοι φτάσουν μια “οικονομικά σημαντική μειοψηφία X ”—μια ομάδα αρκετά μεγάλη ώστε η καταστολή εναντίον της να προκαλεί μη τετριμμένη οικονομική ζημία και η πολιτική ανυπακοή να γίνεται αξιόπιστη απειλή—το κράτος εισέρχεται σε διαπραγμάτευση. Για λόγους παραδείγματος, χρησιμοποιούμε $X \approx 15\%$ του ΑΕΠ, αλλά το πραγματικό όριο εξαρτάται από τη συγκεκριμένη οικονομία.

10 Ανάλυση Ασφάλειας

Θεωρούμε πέντε κατηγορίες αντιπάλων: μεμονωμένους κακόβουλους δράστες, οργανωμένες ομάδες, εταιρικούς αντιπάλους, αντιπάλους κρατικού επιπέδου και αντιπάλους επιπέδου πρωτοκόλλου.

Αντίσταση Sybil [12]. Η οικοδόμηση φήμης απαιτεί διαρκή, επαληθεύσιμη αλληλεπίδραση. Το κόστος μιας επιτυχημένης επίθεσης Sybil κλιμακώνεται γραμμικά με τις πλαστές ταυτότητες και τετραγωνικά με το επίπεδο-στόχο φήμης. Η λειτουργία πολλαπλών DIDs παράλληλα είναι δυνατή αλλά δαπανηρή εκ σχεδιασμού—κάθε ταυτότητα πρέπει να συσσωρεύσει φήμη ανεξάρτητα μέσω γνήσιας δραστηριότητας. Στις ελεύθερες κοινωνίες αυτό το κόστος αποτρέπει την ευκαιριακή κατάχρηση· στις δικτατορίες, τα παράλληλα DIDs γίνονται εργαλείο επιβίωσης που

επιτρέπει διαμερισματοποιημένη αντίσταση, υπόγειο συντονισμό και ασφαλέστερη πλοήγηση στη μαύρη αγορά.

Άμυνα κατά της συμπαιγνίας. Μοτίβα αμοιβαίας έγκρισης μεταξύ κλειστών ομάδων είναι ανιχνεύσιμα μέσω ανάλυσης κοινωνικού γράφου. Οι συναρτήσεις συγκέντρωσης φήμης προεξοφλούν τους ισχυρισμούς από στενά συνδεδεμένες πηγές.

Αντίπαλος κρατικού επιπέδου. Η δρομολόγηση οπίου, η απουσία κεντροποιημένης υποδομής και η κατανομή του ρόλου του Επαληθευτή σε όλη τη βάση των συμμετεχόντων εξασφαλίζουν ότι η καταστολή απαιτεί μέτρα δυσανάλογα προς οποιοδήποτε όφελος.

Ιδιωτικότητα έναντι λογοδοσίας. Η ψευδωνυμία—μία μέση οδός μεταξύ ανωνυμίας και αποκάλυψης ταυτότητας—επιτρέπει στα DIDs να συσσωρεύουν ουσιαστική φήμη χωρίς να αποκαλύπτουν την πραγματική ταυτότητα του Κατόχου.

11 Ζητήματα Ιδιωτικότητας

Το μοντέλο ιδιωτικότητας του RSN βασίζεται στην ψευδωνυμία. Ο Κάτοχος ελέγχει την αποκάλυψη της ταυτότητας: ελάχιστη (καθαρό ψευδώνυμο), επιλεκτική (συγκεκριμένα διαπιστευτήρια συνδεδεμένα), ή πλήρη (νομική ταυτότητα συσχετισμένη). Οι δημοσιευμένοι ισχυρισμοί είναι μόνιμοι—το σύστημα υποστηρίζει τη συμφραζόμενη διόρθωση αλλά όχι τη διαγραφή. Ένας Κάτοχος μπορεί να εγκαταλείψει ένα εκτεθειμένο DID και να ξεκινήσει από την αρχή, χάνοντας τη συσσωρευμένη φήμη.

12 Σχετική Εργασία

Η προδιαγραφή W3C DID Core [2] και το Ceramic Network [8] παρέχουν το θεμέλιο της ταυτότητας. Το EigenTrust [13] επέδειξε κατανεμημένη συγκέντρωση φήμης χωρίς κεντρική αρχή. Τα SBTs [3] εισήγαγαν μη μεταβιβάσιμα κοινωνικά tokens. Το RSN διαφέρει στην έμφασή του στο οικονομικό κόστος ως φίλτρο ποιότητας και στον μηχανισμό του για την τιμολόγηση του ριζοσπαστισμού.

Τα DAOs [4] και η τετραγωνική ψηφοφορία [5] επέδειξαν τη σκοπιμότητα της αποκεντρωμένης διακυβέρνησης. Το RSN αντλεί τη συναίνεση από διμερείς διαπραγματεύσεις τιμών αντί για ψηφοφορία.

Η πρόταση αντλεί από την αναρχοκαπιταλιστική θεωρία [14, 15] για την ιδιωτική παροχή υπηρεσιών, αλλά αποκλίνει σε δύο κρίσιμα σημεία: σχεδιάζει

για την κακία και τις τιμωρητικές παρορμήσεις αντί να προϋποθέτει ορθολογισμό, και προτείνει σταδιακή μετάβαση αντί για επανάσταση. Η έννοια των αναδυόμενων κοινωνικών συμβολαίων έχει προηγούμενα στη θεωρία της αυθόρμητης τάξης του Hayek [16].

Αναρχο-αγορισμός. Το RSN μοιράζεται σημαντικό κοινό έδαφος με την αγοριστική αντι-οικονομία [17]—ιδιαίτερα την έμφαση στην οικοδόμηση παράλληλων θεσμών και στην εθελοντική ανταλλαγή. Ωστόσο, ο αγορισμός τείνει να προϋποθέτει το ορθολογικό ιδιοτελές συμφέρον ως επαρκή μηχανισμό συντονισμού και συχνά στερείται μιας συγκεκριμένης διαδρομής μετάβασης από τις υπάρχουσες κρατικές δομές. Το RSN ενσωματώνει ρητά μη ορθολογικές συμπεριφορικές τάσεις και παρέχει έναν μηχανισμό δημοσιονομικής πίεσης για σταδιακή μετάβαση.

Αξιοκρατία. Το RSN μπορεί να αντιπροσωπεύει μια πρώτη λειτουργική περιγραφή του πώς η αξιοκρατία [18] μπορεί να αναδυθεί ως συστημική ιδιότητα αντί για σύνθημα. Τα παραδοσιακά αξιοκρατικά συστήματα αποτυγχάνουν επειδή απαιτούν μια κεντρική αρχή να ορίσει και να επιβάλει την “αξία”. Στο RSN, η αξία αναδύεται από διμερείς αξιολογήσεις: όσοι προσφέρουν αξία συσσωρεύουν φήμη· καμία επιτροπή δεν αποφασίζει ποιος έχει αξία.

Η ιδιοκτησία ως προνόμιο. Το RSN αποκλίνει θεμελιωδώς από τις αναρχοκαπιταλιστικές και αυστριακής σχολής προσεγγίσεις των δικαιωμάτων ιδιοκτησίας ως φυσικών και απόλυτων. Στο πλαίσιο του RSN, η ιδιοκτησία είναι *προνόμιο*—μία κοινωνική αναγνώριση που μπορεί, σε ακραίες περιπτώσεις, να ανακληθεί από την κοινότητα όταν ένας συμμετέχων παραβιάζει θεμελιωδώς τις κοινές νόρμες (προδοσία, άρνηση υπεράσπισης της κοινότητας σε υπαρξιακή κρίση, συστηματική εκμετάλλευση). Αυτό δεν είναι κρατική απαλλοτρίωση αλλά ανάκληση της κοινωνικής αναγνώρισης από το δίκτυο των διμερών σχέσεων.

13 Συζήτηση και Περιορισμοί

Ψυχρή εκκίνηση. Η αξία του RSN εξαρτάται από τα φαινόμενα δικτύου· οι πρώτοι χρήστες αντιμετωπίζουν περιορισμένη αξία μέχρι η συμμετοχή να φτάσει ένα όριο. Ωστόσο, ακόμη και από τα πρώτα στάδια, το δίκτυο DID χρησιμεύει ως χρήσιμη συμπληρωματική πηγή πληροφοριών. Η πρόωπη αξιολόγηση φήμης και η εκτίμηση αρχών αναμένεται να αναπτυχθούν σταδιακά με αυξανόμενη πολυπλοκότητα.

Αντι-παρασιτισμός και έλεγχος πρόσβασης.

Τα στοχευμένα DIDs μπορούν να επιβάλουν διαβαθμισμένα τέλη και περιορισμούς πρόσβασης σε ερωτήματα από DIDs χαμηλής φήμης. Αυτό δεν είναι δυαδικό αλλά μια συνεχής κλίμακα: όσο λιγότερη φήμη έχει ένα ερωτών DID, τόσο λιγότερη πληροφορία λαμβάνει, τόσο περισσότερο περιμένει και τόσο περισσότερο πληρώνει. Αυτός ο μηχανισμός δίνει κίνητρο για γνήσια συμμετοχή αντί για παθητική κατανάλωση.

Ανισότητα πρόσβασης. Το κόστος δημοσίευσης ισχυρισμών μπορεί να φιλτράρει νόμιμα παράπονα από οικονομικά μειονεκτούντες συμμετέχοντες. Μετριασμός: κάθε συμμετέχων χρησιμεύει ταυτόχρονα ως δυνητικός επαλήθευτής (ή αναθέτει αυτόν τον ρόλο) και κερδίζει τέλη επαλήθευσης. Σε επαρκή χρονικό ορίζοντα, ένας μη ριζοσπαστικός συμμετέχων θα πρέπει να προσεγγίσει τη χρηματοοικονομική ουδετερότητα—με το εισόδημα από την επαλήθευση να αντισταθμίζει περίπου το κόστος δημοσίευσης. Αυτή είναι μια στατιστική προσδοκία, όχι εγγύηση.

Ανισότητα φήμης. Οι πρώτοι χρήστες συσσωρεύουν πλεονεκτήματα που μπορεί να δημιουργήσουν εμπόδια για τους μεταγενέστερους. Ωστόσο, η αξιολόγηση φήμης εκτελείται από τρίτους παρόχους που μπορούν να επιλέξουν να μετριάσουν το πλεονέκτημα του πρωτοπόρου μέσω των αλγορίθμων συγκέντρωσής τους. Το να είσαι πρώτος με καλή φήμη είναι ένα νόμιμο συγκριτικό οικονομικό πλεονέκτημα—και αυτό είναι εκ σχεδιασμού.

Ανοιχτά ερωτήματα. Οι βέλτιστες συναρτήσεις κόστους, τα πρότυπα συγκέντρωσης, η διακυβέρνηση του πρωτοκόλλου και η αλληλεπίδραση με συνθετικά δεδομένα φήμης παραγόμενα από TN παραμένουν πεδία για μελλοντική εργασία.

Η παρούσα εργασία δεν ισχυρίζεται ότι το RSN θα παράγει βέλτιστα αποτελέσματα σε όλες τις περιστάσεις. Ισχυρίζεται ότι το RSN αντιπροσωπεύει μια *εφικτή* εναλλακτική—τεχνικά υλοποιήσιμη, οικονομικά αυτοσυντηρούμενη, και κοινωνικά συμβατή με τις ανθρώπινες συμπεριφορικές τάσεις όπως πραγματικά είναι.

14 Συμπέρασμα

Η παρούσα εργασία παρουσίασε το Κοινωνικό Δίκτυο Φήμης, ένα αποκεντρωμένο πρωτόκολλο που επιτρέπει ψευδώνυμη, επαληθεύσιμη ανταλλαγή φήμης. Η Αρχή του Ακριβούς Ριζοσπαστισμού διασφαλίζει ότι οι δόλιοι ισχυρισμοί τιμολογούνται εκτός αγοράς χωρίς λογοκρισία. Η προτεινόμενη διαδρομή μετάβασης επιτρέπει σταδιακή,

αναστρέψιμη μετάβαση από τους υπάρχοντες θεσμούς. Ο σχεδιασμός ενσωματώνει την ανθρώπινη φύση όπως είναι—συμπεριλαμβανομένης της μικροπρέπειας, της κακίας και της επιθυμίας για τιμωρητική ικανοποίηση—αντί να απαιτεί ιδεολογικό μετασχηματισμό. Το αποτέλεσμα δεν είναι ουτοπία αλλά ένα σύστημα όπου η δικαιοσύνη είναι προσβάσιμη, η φήμη κερδίζεται, και το κόστος της κακής συμπεριφοράς το επωμίζεται το μέρος που την προκάλεσε.

References

- [1] Czech Republic, “Act no. 549/1991 coll., on court fees, as amended,” 1991, fee schedule for court proceedings; cost rules per Act No. 99/1963 Coll. (Code of Civil Procedure) and Decree No. 177/1996 Coll. (Attorney Tariff).
- [2] M. Sporny, D. Longley, M. Sabadello, D. Reed, O. Steele, and C. Allen, “Decentralized identifiers (DIDs) v1.0,” W3C Recommendation, Jul. 2022.
- [3] E. G. Weyl, P. Ohlhaber, and V. Buterin, “Decentralized society: Finding Web3’s soul,” *SSRN Electronic Journal*, May 2022.
- [4] V. Buterin, “DAOs, DACs, DAs and more: An incomplete terminology guide,” Ethereum Blog, May 2014.
- [5] V. Buterin, Z. Hitzig, and E. G. Weyl, “A flexible design for funding public goods,” *Management Science*, vol. 65, no. 11, pp. 5171–5187, 2019.
- [6] D. Karger, E. Lehman, T. Leighton, R. Panigrahy, M. Levine, and D. Lewin, “Consistent hashing and random trees: Distributed caching protocols for relieving hot spots on the World Wide Web,” in *Proc. 29th ACM STOC*, 1997, pp. 654–663.
- [7] D. Buchner, “ION — a scalable DID method based on Bitcoin,” Microsoft, 2021.
- [8] Ceramic Network, “Ceramic protocol specification,” GitHub, 2023. [Online]. Available: <https://github.com/ceramicnetwork>
- [9] É. Durkheim, *The Division of Labor in Society*. Free Press, 1893, english translation 1984.
- [10] J. Rawls, *A Theory of Justice*. Harvard University Press, 1971.

- [11] J. Haidt, *The Righteous Mind: Why Good People Are Divided by Politics and Religion*. Vintage Books, 2012.
- [12] J. R. Douceur, “The Sybil attack,” in *Proc. 1st International Workshop on Peer-to-Peer Systems (IPTPS)*, 2002, pp. 251–260.
- [13] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, “The EigenTrust algorithm for reputation management in P2P networks,” in *Proc. 12th International Conference on World Wide Web*, 2003, pp. 640–651.
- [14] M. N. Rothbard, *For a New Liberty: The Libertarian Manifesto*. Macmillan, 1973.
- [15] H.-H. Hoppe, *Democracy: The God That Failed*. Transaction Publishers, 2001.
- [16] F. A. Hayek, *Law, Legislation and Liberty*. University of Chicago Press, 1973.
- [17] S. E. I. Konkin, *An Agorist Primer*. KoPubCo, 2006.
- [18] M. Young, *The Rise of the Meritocracy*. Thames and Hudson, 1958.