

विकेंद्रीकृत प्रतिष्ठा नेटवर्क: स्वाभाविक सामाजिक संगठन का एक ढाँचा

Pavel Kudrna
Prague, Czechia
प्रारूप v1 — मार्च 2026

Abstract

न्याय की भावना—यह विश्वास कि अन्याय का प्रतिकार होता है और योग्यता को पुरस्कृत किया जाता है—समाज की सबसे प्रबल संगठक शक्ति है। जब शासन की केंद्रीकृत संस्थाएँ यह भावना प्रदान नहीं कर पाती क्योंकि किसी अधिकार को लागू करने की लागत स्वयं उस अधिकार के मूल्य से अधिक हो जाती है, तब सामाजिक एकजुटता क्षरित होने लगती है। वर्तमान संस्थागत संरचनाएँ विवादों के एक बड़े वर्ग को व्यवस्थित रूप से उसी तरह हल करने में विफल रहती हैं जैसे केंद्रीय नियोजन संसाधनों का आवंटन करने में विफल रहता है: सूचना की असमानता, अनुपस्थित फीडबैक चक्रों, और निर्णयकर्ताओं का उनके निर्णयों के परिणामों से विच्छेदन के माध्यम से। यह शोधपत्र एक प्रतिष्ठा सामाजिक नेटवर्क (RSN) प्रस्तुत करता है: विकेंद्रीकृत पहचानकर्ताओं (DIDs) पर निर्मित एक विकेंद्रीकृत, अभ्रष्ट, सेंसरशिप-प्रतिरोधी संचार परत, जो छद्मनामी प्रतिभागियों को वास्तविक-जगत के व्यवहार के बारे में प्रतिष्ठा सूचना प्रकाशित करने, सत्यापित करने और उपभोग करने में सक्षम बनाती है। मूल तंत्र तीन डिज़ाइन सिद्धांतों पर टिका है: (1) एक असममित लागत संरचना जहाँ प्रतिष्ठा डेटा पढ़ना सस्ता है परंतु लिखने के लिए सत्यापन-योग्य प्रयास आवश्यक है; (2) संगत हैशिंग पर आधारित एक अनिर्धारक सत्यापनकर्ता चयन प्रोटोकॉल जो बढ़ती हुई पुनरावृत्ति लागतों के माध्यम से आमूल दावों की कीमत तय करता है; और (3) एक बाज़ार-चालित प्रतिष्ठा प्राधिकरण मॉडल जहाँ निजी सत्यापनकर्ता उन दावों की सटीकता पर अपनी संचित प्रतिष्ठा दाँव पर लगाते हैं जिनका वे समर्थन करते हैं। परिणामी वास्तुकला बिना केंद्रीय समन्वय के उदीयमान योग्यतातंत्र उत्पन्न करती है और मौजूदा राज्य-प्रशासित व्यवस्थाओं से एक क्रमिक, प्रतिवर्ती स्थानांतरण मार्ग को सक्षम बनाती है।

1 परिचय

1.1 केंद्रीकृत विश्वास की समस्या

आधुनिक शासन एक मूलभूत धारणा पर टिका है: कि केंद्रीकृत संस्थाएँ बड़े पैमाने पर अजनबियों के बीच विश्वास की मध्यस्थता कर सकती हैं। अदालतें विवादों का निपटारा करती हैं। रजिस्ट्रियाँ स्वामित्व को प्रमाणित करती हैं। नियामक निकाय मानकों को लागू करते हैं। ये संस्थाएँ एक ऐसे युग में गढ़ी गई थीं

जब सूचना दुर्लभ थी, संचार धीमा था, और किसी केंद्रीय निकाय को अधिकार का प्रत्यायोजन ही एकमात्र व्यवहार्य समन्वय तंत्र था। तथापि केंद्रीकृत शासन उन्हीं संरचनात्मक कारणों से विफल होता है जिनसे केंद्रीय नियोजन विफल होता है: सूचना की असमानता, अनुपस्थित फीडबैक चक्र, और निर्णयकर्ताओं का उनके निर्णयों के परिणामों से विच्छेदन।

यह धारणा तब विफल हो जाती है, उदाहरण के लिए, जब संस्थागत मध्यस्थता की लागत विवाद के मूल्य से अधिक हो जाती है। एक किरायेदार पर विचार कीजिए जिसे पता चलता है कि उसके किराए के अपार्टमेंट में कानूनन आवश्यक विद्युत सुरक्षा प्रमाणपत्र नहीं है—एक ऐसी स्थिति जो जीवन के लिए तत्काल खतरा उत्पन्न करती है। अनुबंध से हटने का किरायेदार का कानूनी अधिकार असंदिग्ध है। फिर भी उस अधिकार को अदालती व्यवस्था के माध्यम से लागू करने की लागत जमानत राशि और देय क्षतिपूर्ति के मौद्रिक मूल्य से अधिक होती है, यहाँ तक कि संभावित वैधानिक मुआवजे को शामिल करने पर भी [1]। तर्कसंगत प्रतिक्रिया यह है कि हानि को सहन कर लिया जाए और बाहर निकल लिया जाए।

यह कोई रोगात्मक अपवाद नहीं है। यह विवादों के एक बड़े वर्ग का सामान्य अनुभव है जिनमें हानि वास्तविक है परंतु मौद्रिक दाँव उस दहलीज़ से नीचे रहता है जिस पर संस्थागत प्रवर्तन आर्थिक रूप से तर्कसंगत बनता है। परिणाम एक ऐसी व्यवस्था है जो संरचनात्मक रूप से दुष्ट अभिकर्ताओं का पक्ष लेती है: जो लोग दूसरों को इस दहलीज़ से कम मात्रा में हानि पहुँचाते हैं, वे दंडमुक्ति के साथ कार्य कर सकते हैं, क्योंकि न्याय पाने की लागत पीड़ित पक्ष पर पड़ती है।

उपर्युक्त उदाहरण लेखक के कानूनी परिवेश—चेक नागरिक-कानून व्यवस्था—से लिया गया है। अन्य कानूनी परंपराओं में—पूर्वनिर्णय-आधारित सामान्य कानून, प्रथागत कानून, मिश्रित व्यवस्थाएँ—न्याय अलग-अलग ढंग से और अलग-अलग मात्रा में विफल होता है, जो उस क्षेत्राधिकार की सांस्कृतिक और प्रक्रियात्मक विशिष्टताओं पर निर्भर करता है। पाठक संभवतः अपने संदर्भ से समान उदाहरण पहचान लेंगे। जो संरचनात्मक रूप से सार्वभौमिक है वह है यह पैटर्न: वे विवाद जिनका मूल्य आर्थिक रूप से तर्कसंगत प्रवर्तन की दहलीज़ से नीचे आता है, इस तरह समाप्त होते हैं कि हानि पीड़ित पक्ष द्वारा सह ली जाती है। RSN पूर्ण न्याय का वादा नहीं करता—यह केवल उस संरचनात्मक लाभ को घटाता है जो दुष्ट अभिकर्ताओं को तब मिलता है जब संस्थागत प्रवर्तन अलाभकारी होता है।

1.2 मौजूदा समाधान क्यों अपर्याप्त हैं

विकेंद्रीकृत पहचान (DID) ढाँचे [2] स्व-संप्रभु पहचान प्रबंधन के लिए क्रिप्टोग्राफिक तंत्र प्रदान करते हैं परंतु मुख्यतः पहचान सत्यापन पर केंद्रित रहते हैं, व्यवहारगत प्रतिष्ठा के व्यापक प्रश्न को संबोधित किए बिना।

सोलबाउंड टोकन (SBTs) [3] इस अंतर्दृष्टि को पकड़ते हैं कि प्रतिष्ठा अहस्तांतरणीय है, परंतु मापनीयता की बाधाओं वाले ब्लॉकचेन अवसंरचना पर निर्भर करते हैं और सूचना प्रविष्टि को नियंत्रित करने वाले आर्थिक प्रोत्साहनों को संबोधित नहीं करते। संबंधित अवधारणाएँ जैसे मेरिट टोकन (उदा., Liberland) समान दर्शन साझा करती हैं परंतु विशिष्ट क्षेत्राधिकार ढाँचों से बंधी रहती हैं।

विकेंद्रीकृत स्वायत्त संगठन (DAOs) [4] स्मार्ट अनुबंधों के माध्यम से शासन को क्रियान्वित करते हैं परंतु धनिकतंत्रीय गतिशीलता की पुनरावृत्ति करते हैं जहाँ प्रभाव पूँजी के अनुपात में होता है। द्विघातीय मतदान [5] इसे आंशिक रूप से कम करता है परंतु व्यावहारिक अपनाव को सीमित करता है। DAOs मूलभूत ओरैकल समस्या का भी सामना करते हैं: स्मार्ट अनुबंध किसी विश्वसनीय बाहरी स्रोत के बिना वास्तविक-जगत की स्थितियों को विश्वसनीय ढंग से सत्यापित नहीं कर सकते, और इस समस्या का ब्लॉकचेन वास्तुकला के भीतर कोई सामान्य समाधान नहीं है।

कोई भी मौजूदा व्यवस्था विकेंद्रीकरण, सेंसरशिप प्रतिरोध, छद्मनामिता, प्रवेश की सत्यापन-योग्यता, और उदीयमान सहमति को एक साथ नहीं जोड़ती।

1.3 योगदान

यह शोधपत्र निम्नलिखित योगदान करता है:

1. **प्रतिष्ठा सामाजिक नेटवर्क (RSN)** की परिभाषा, एक विकेंद्रीकृत प्रोटोकॉल जो द्विपक्षीय प्रतिष्ठा विनियम का समर्थन करने के लिए DID ढाँचे का विस्तार करता है।
2. संगत हैशिंग पर आधारित एक **अनिर्धारक सत्यापनकर्ता चयन प्रोटोकॉल** [6]।
3. **महँगे आमूलवाद का सिद्धांत**, जो दावों की कीमत नेटवर्क सहमति से उनकी दूरी के अनुसार तीन संयुक्त लागत चैनलों के माध्यम से तय करता है।
4. असममित प्रोत्साहनों वाला एक **प्रतिष्ठित प्राधिकरण मॉडल** जहाँ मिथ्या समर्थन की लागत वैध शुल्क से अत्यधिक भयावह रूप से अधिक होती है।
5. समानांतर राजकोषीय अवसंरचना के माध्यम से एक **क्रमिक स्थानांतरण मार्ग**।

2 डिज़ाइन सिद्धांत

RSN वास्तुकला पाँच गैर-परक्राम्य डिज़ाइन सिद्धांतों से अनुबद्ध है।

निरंतरता और विकास। यह व्यवस्था अनिश्चित अवधि के संक्रमण-काल के दौरान मौजूदा संस्थाओं के साथ सह-अस्तित्व

में रहती है। संक्रमण हर चरण पर प्रतिवर्ती होना चाहिए।

स्वैच्छिकता और उत्तरदायित्व। भागीदारी स्वैच्छिक है, परंतु स्वैच्छिकता उत्तरदायित्व से युग्मित है: जो प्रतिभागी किसी संस्थागत कार्य पर नियंत्रण ग्रहण करता है, वह साथ ही उससे जुड़े दायित्वों को भी ग्रहण करता है।

विविधता और सांस्कृतिक तटस्थता। सहमति द्विपक्षीय अंतःक्रियाओं से उभरती है, न कि व्यवस्था के रचयिताओं द्वारा थोपे गए पूर्वनिर्धारित नियमों से।

लचीलापन और सेंसरशिप प्रतिरोध। नेटवर्क को सेंसर करने की लागत उसे सहन करने की लागत से अधिक होनी चाहिए। केवल पूर्ण अधिनायकवाद—विनाशकारी राजनीतिक और आर्थिक लागत पर—इस व्यवस्था को दबा सकता है।

सहमति और प्रवर्तन। यह व्यवस्था क्षुद्रता, द्वेष और प्रतिशोधात्मक संतुष्टि की मानवीय प्रवृत्तियों को भार-वहन करने वाली विशेषताओं के रूप में समाहित करती है। दुराचार निषिद्ध नहीं है; उसकी कीमत तय की जाती है।

3 व्यवस्था का सिंहावलोकन

3.1 प्रतिष्ठा सामाजिक नेटवर्क

RSN एक विकेंद्रीकृत, सम-से-सम (peer-to-peer) संचार परत है जिसमें प्रतिभागी वास्तविक-जगत के व्यवहार के बारे में सत्यापन-योग्य सूचना का आदान-प्रदान करते हैं। इसके परिभाषक गुण हैं: विकेंद्रीकृत और असेंसरणीय अवसंरचना; DIDs के माध्यम से छद्मनामी भागीदारी; असममित लागत संरचना (पढ़ना सस्ता है, लिखना महंगा है); क्रिप्टोग्राफिक सत्यापन-योग्यता; और **मानक समर्थन**—नेटवर्क के माध्यम से प्रसारित सूचना के लिए, प्राधिकरणों द्वारा प्रस्तुत सेवाओं के लिए (दावा रचना, समर्थन, साक्षी सेवा), तथा नीति प्रारूप के लिए मशीन-पठनीय स्वरूप, जिसमें प्रतिपक्ष की प्रतिष्ठा का मूल्यांकन करने और नीति-असंगति (घोषित और वास्तविक व्यवहार के बीच) के जोखिम का आकलन करने के नियम शामिल हैं।

3.2 वास्तुशिल्पीय घटक

RSN चार प्रमुख घटकों से मिलकर बना है (चित्र 1):

1. **DID परत।** घोषित नियमों, प्रतिष्ठा मेटाडेटा, और नेटवर्क रूटिंग के साथ प्रतिभागी पहचानें।
2. **दावा प्रोटोकॉल।** वास्तविक-जगत की घटनाओं के बारे में अभिकथन प्रकाशित करने के लिए संरचित स्वरूप।
3. **सत्यापन नेटवर्क।** संगत हैशिंग का उपयोग करके सत्यापनकर्ताओं को नियुक्त करने के लिए विकेंद्रीकृत प्रोटोकॉल।
4. **प्रतिष्ठा समुच्चयन परत।** मानव-पठनीय प्रतिष्ठा सारांश उत्पन्न करने वाली सेवाएँ।

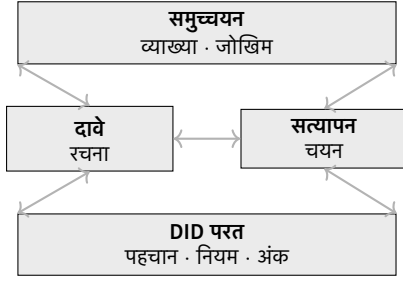


Figure 1: RSN चार-परत वास्तुकला।

3.3 प्रतिभागी भूमिकाएँ

एक सत्यापन लेनदेन में छह तक विशिष्ट DID भूमिकाएँ शामिल होती हैं (चित्र 2): **जारीकर्ता** (DID_I , दावा रचना और प्रस्तुत करता है), **विषय** (DID_S , वह DID जिसके बारे में दावा है—जारीकर्ता के साथ अभिन्न हो सकता है), **प्राधिकरण** (DID_A , शुल्क के बदले दावे का समर्थन करता है; साक्षी सेवाएँ भी प्रस्तुत कर सकता है—वैकल्पिक), **साक्षी** ($DID_{W1..n}$, चुनौती-कोडों के माध्यम से सत्यापनकर्ता की ईमानदारी का गुप्त निरीक्षक—वैकल्पिक), **सत्यापनकर्ता** (DID_V , दावा प्रकाशित करने के लिए एल्गोरिदमिक रूप से चयनित), और **RSN** (वह नेटवर्क जहाँ सत्यापित दावे प्रकाशित होते हैं)। कोई भी भूमिका किसी अन्य DID को प्रत्यायोजित की जा सकती है (खंड 7.4)। एक प्राधिकरण सामान्यतः समर्थन को साक्षी सेवाओं के साथ बंडल करता है, परंतु दोनों कार्य तार्किक रूप से स्वतंत्र हैं।

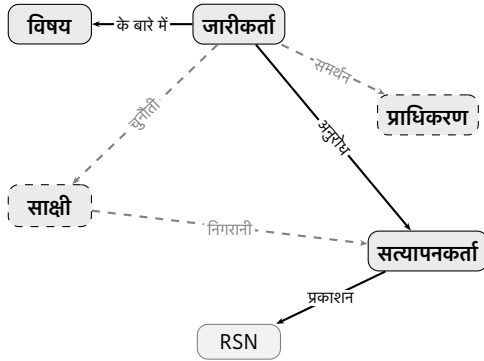


Figure 2: सत्यापन लेनदेन में DID भूमिकाएँ। धराशायी = वैकल्पिक (प्राधिकरण, साक्षी)।

3.4 अभ्रष्टता: चार शक्तियाँ

RSN की अभ्रष्टता किसी एकल तंत्र से नहीं बल्कि चार समवर्ती शक्तियों से उत्पन्न होती है। कोई भी अकेले पर्याप्त नहीं है; केवल उनका संयोजन ही भ्रष्टाचार के प्रयास को आर्थिक रूप से अतार्किक बनाता है।

अप्रत्याशित लक्ष्य। प्रत्येक दावे के लिए सत्यापनकर्ता को संगत हैशिंग के माध्यम से अनिवार्य रूप से चुना जाता है (खंड 5.3)। एक हमलावर घूस के लिए किसी विशिष्ट सत्यापनकर्ता को पूर्व-लक्षित नहीं कर सकता, क्योंकि सत्यापनकर्ता की पहचान दावे की सामग्री और पिछली

पुनरावृत्तियों का फलन है, न कि जारीकर्ता के चयन का।

प्रतिष्ठागत उत्तोलन—धीमे ऊपर, तेज़ नीचे। प्रतिष्ठा केवल क्रमिक रूप से, सतत सुसंगत व्यवहार के माध्यम से अर्जित की जा सकती है। तथापि यह एक ही कपटपूर्ण समर्थन में भयावह रूप से गँवाई जा सकती है (खंड 6.2)। इस असममितता का अर्थ है कि वर्षों की संचित प्रतिष्ठा एक बेईमान समर्थन से नष्ट हो सकती है; इष्टतम रणनीति संदिग्ध दावों को अस्वीकार करना ही रहती है।

सार्वजनिक वचन। प्रत्येक DID धारक सार्वजनिक रूप से अपनी नीति घोषित करता है—नियमों का एक मशीन-पठनीय समुच्चय जिसका पालन करने के लिए वह प्रतिबद्ध होता है। घोषणा और वास्तविक व्यवहार के बीच का विचलन पहचाने जाने योग्य है और मूल उल्लंघन से भी अधिक गंभीर प्रतिष्ठागत अपराध के रूप में उसकी कीमत तय की जाती है (खंड 7.3)। इसलिए पाखंड प्रत्यक्ष बेईमानी से अधिक महंगा है।

जाल आक्रमण-लागत असममितता। नेटवर्क को सेंसर या अस्थिर करने की लागत नेटवर्क के आकार और घनत्व के साथ अरैखिक रूप से बढ़ती है, जबकि उसे सहन करने की लागत स्थिर रहती है। सेंसरशिप को लाभदायक बनाने के लिए किसी केंद्रीकृत अभिकर्ता को उसे पूरे नेटवर्क पर लागू करना होगा—जिसके लिए किसी भी कल्पनीय लाभ की तुलना में असमानुपातिक उपाय आवश्यक होंगे (खंड 10)।

4 विकेंद्रीकृत पहचान मॉडल

4.1 विशेष गुणों वाला DID

RSN, W3C DID Core विशिष्टि [2] का विस्तार निम्नलिखित के साथ करता है: **घोषित नियम** (मशीन-पठनीय व्यवहारगत प्रतिबद्धताएँ), **प्रतिष्ठा मेटाडेटा** (समुच्चयित व्यवहारगत अंक), और **नेटवर्क रूटिंग** (स्थिर रिंग स्थिति से पृथक परिवर्तनशील ओनियन गेटवे)।

4.2 दावे का जीवनचक्र

एक दावा छह चरणों से होकर गुजरता है (चित्र 3): रचना, वैकल्पिक प्राधिकरण समर्थन, संगत हैशिंग के माध्यम से सत्यापनकर्ता चयन, सत्यापन निर्णय (स्वीकार या पुनरावृत्ति के साथ अस्वीकार), प्रकाशन, और सभी पक्षों के लिए प्रतिष्ठा अद्यतन।

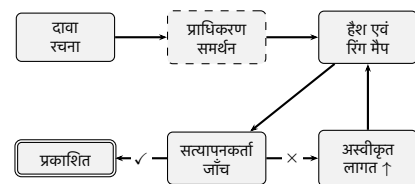


Figure 3: पुनरावृत्ति चक्र के साथ दावे का जीवनचक्र।

4.3 W3C DID Core से संबंध

RSN का पहचान मॉडल W3C DID Core विशिष्टि [2] का एक उचित अधिसमुच्चय है। सभी RSN DIDs वैध W3C DIDs हैं। RSN-वशिष्टि विस्तार एक समर्पित DID विधि विशिष्टि में परिभाषित DID दस्तावेज गुणों के रूप में संकेतित किए जाते हैं, जो ION [7] और Ceramic [8] जैसी मौजूदा अवसंरचना के साथ संगत हैं।

5 सूचना सत्यापन और प्रसार

5.1 सूचना प्रविष्टि की लागत

RSN का मूल आर्थिक सिद्धांत पढ़ने और लिखने के बीच की असममितता है। DID नेटवर्क का हिस्सा बने और अपनी प्रतिष्ठा के अनुरूप पहुँच रखने वाले प्रतिभागियों के लिए प्रतिष्ठा डेटा पढ़ना शून्य सीमांत लागत के करीब पहुँचता है—नवागंतुकों को क्रमशः व्यापक पहुँच अर्जित करनी होती है (देखें एंटी-लीचिंग)। लिखना—जिसे नेटवर्क में प्रतिष्ठा के स्थायी मूर्तिकरण के रूप में समझा जाता है, न कि एक बार के तकनीकी कार्य के रूप में—के लिए तीन आयामों में सत्यापन-योग्य संचयी निवेश आवश्यक है: **समय** (सुसंगत व्यवहार, पूर्ण की गई प्रतिबद्धताओं और सँवारे गए संबंधों में व्यतीत जीवन के वर्ष), **ऊर्जा** (ईमानदार व्यवहार, साझेदारियों की देखभाल और दीर्घकालिक विश्वसनीयता में लगाया गया प्रयास), और **धन** (अपने नाम में निवेश—पेशेवर विकास, अपने कार्य की गुणवत्ता, पहुँचाई गई हानियों का प्रतिकरण)। प्रतिष्ठा तत्काल नहीं खरीदी जा सकती—यह आजीवन संचयन का परिणाम है जिसे व्यवस्था मात्र दृश्यमान बनाती है और संदर्भों में स्थानांतरणीय बनाती है। प्रोटोकॉल की एक बार की तकनीकी लागतें (क्रिप्टोग्राफिक हस्ताक्षर, सत्यापनकर्ता शुल्क) इस अंतर्निहित निवेश की तुलना में नगण्य हैं।

5.2 सामाजिक आलेख और संपर्क गहराई

RSN मूलतः एक सामाजिक नेटवर्क है: प्रत्येक DID उन संपर्कों (अन्य DIDs) को जोड़ता है जो कनेक्शन की अनुमति देते हैं। इन संपर्कों के अपने संपर्क होते हैं, और इसी तरह आगे। एल्गोरिदमिक सत्यापनकर्ता खोज जुड़े हुए संपर्कों की एक विन्यास-योग्य गहराई h के भीतर संचालित होती है (उदा., $h = 3$: किसी के प्रत्यक्ष संपर्क, उनके संपर्क, और संपर्कों के संपर्क)। इस वास्तुकला के लिए एकल वैश्विक ब्लॉकचेन आवश्यक नहीं है—यह स्वाभाविक रूप से अन्य समुदायों में अतिच्छादन वाले समुदायों/समूहों के उद्भव का पक्ष लेती है। प्रत्येक DID प्रतिभागी की एक प्रकाशित नीति होनी चाहिए—नियमों का एक मशीन-पठनीय समुच्चय जो नियंत्रित करता है कि आने वाले अनुरोधों का मूल्यांकन कैसे किया जाए। नीति उल्लंघन नेटवर्क में नकारात्मक कलाकृतियों के रूप में दर्ज किए जाते हैं।

5.3 एल्गोरिदमिक सत्यापनकर्ता चयन

सत्यापन प्रोटोकॉल संगत हैशिंग का उपयोग करता है [6] (चित्र 4)। सत्यापन एक सशुल्क सेवा है: सत्यापनकर्ता शुल्क के बदले काम करते हैं, जिससे एक ऐसा बाज़ार बनता है जहाँ प्रतिस्पर्धा मूल्य निर्धारण, गति और विश्वसनीयता को संचालित करती है।

चरण 1. दावा दस्तावेज को पिछली पुनरावृत्ति के हैश परिणाम (या पहली पुनरावृत्ति पर $\emptyset$) के साथ संयोजित करके हैश किया जाता है:

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

एल्गोरिदम में सभी पिछले अनुरोधों और प्रतिक्रियाओं का संपूर्ण पथ शामिल होना चाहिए—केवल पिछली पुनरावृत्ति का हैश नहीं। प्रत्येक सत्यापनकर्ता की पूर्ण प्रतिक्रिया (स्वीकृति, अस्वीकृति, उद्धृत मूल्य, कारण) बढ़ते हुए दस्तावेज में जोड़ी जाती है, जो प्रत्येक चरण पर क्रिप्टोग्राफिक हस्ताक्षरों के माध्यम से सत्यापन-योग्य होती है।

चरण 2. हैश को संगत हैश रिंग पर N स्थितियों पर मैप किया जाता है, समान रूप से वितरित (उदा., $N = 4$ के लिए: $+0^\circ, +90^\circ, +180^\circ, +270^\circ$)। प्रत्येक स्थिति से, एक दक्षिणावर्त खोज निकटतम DID को सत्यापनकर्ता उम्मीदवार के रूप में चुनती है (चित्र 5)। N एक परिवर्तनशील पैरामीटर है जो वर्तमान में सक्रिय DIDs के प्रतिशत, दिन के समय, या ऐतिहासिक नेटवर्क प्रतिक्रियाशीलता पर निर्भर कर सकता है।

चरण 3. सत्यापनकर्ता स्वीकार करता है (प्रकाशित करता है, प्रतिष्ठा दाँव पर लगाते हुए) या अस्वीकार करता है (अस्वीकृति हैश के साथ चरण 1 पर लौटते हुए)। जब कोई नोड ऑनलाइन स्थिति घोषित करने के बावजूद प्रतिक्रिया नहीं देता, तो अगले अनुरोध में सभी N पिछले सत्यापनकर्ता उम्मीदवारों की सभी प्रतिक्रियाएँ शामिल होनी चाहिए।

एंटी-लीचिंग। लक्ष्य DIDs कम प्रतिष्ठा वाले नए DIDs से आने वाले प्रश्नों के लिए शुल्क या पहुँच प्रतिबंध निर्धारित कर सकते हैं। यह क्रमिक तंत्र (द्विआधारी नहीं) नवागंतुकों को दूसरों का डेटा स्वतंत्र रूप से उपभोग करने से पहले वास्तविक गतिविधि के माध्यम से प्रतिष्ठा बनाने के लिए बाध्य करता है।

प्रत्येक अस्वीकृति सत्यापनकर्ता की पूर्ण प्रतिक्रिया (कारणों और शर्तों सहित) को दावा दस्तावेज में जोड़ती है, जिससे उसकी सामग्री विस्तृत होती है। विस्तारित दस्तावेज से एक नया हैश अनिवार्य रूप से परिकलित होता है, जो एक भिन्न रिंग स्थिति पर मैप होता है और एक भिन्न सत्यापनकर्ता को चुनता है। संपूर्ण पथ का प्रलेखन अनिवार्य है—जारीकर्ता अगले सत्यापनकर्ता की भविष्यवाणी या उसे प्रभावित नहीं कर सकता। यदि कोई सत्यापनकर्ता संगत घोषित नीति के बावजूद अनुरोध की उपेक्षा करता है, तो साक्षी (यदि उपस्थित हों) इसे दर्ज करते हैं, और जारीकर्ता अंतिम प्रकाशन पर साक्षी साक्ष्य संलग्न कर सकता है।

5.4 साक्षी प्रोटोकॉल

साक्षी भूमिका एक क्रिप्टोग्राफिक चुनौती-कोड प्रोटोकॉल के माध्यम से सत्यापनकर्ता की ईमानदारी के लिए गुप्त जवाबदेही

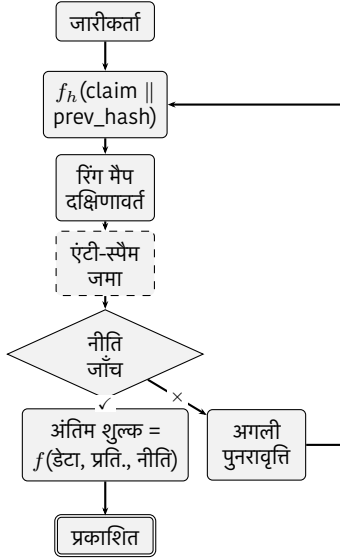


Figure 4: सत्यापनकर्ता चयन प्रोटोकॉल। एंटी-स्पैम जमा वैकल्पिक है और वापसी-योग्य हो सकती है। अंतिम शुल्क केवल स्वीकृति पर ही चुकाया जाता है।

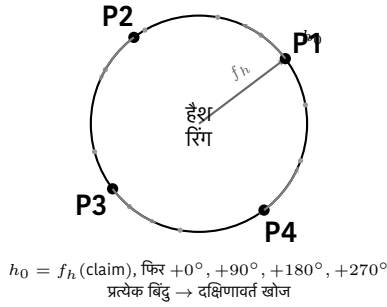


Figure 5: बहु-बिंदु चयन ($N=4$)। हैश h_0 ऑफ़सेट तय करता है; h_0 से समान रूप से वितरित 4 बिंदु।

प्रदान करती है:

चरण W1. अनुरोधकर्ता सत्यापन अनुरोध पर हस्ताक्षर करता है और उसे N_w साक्षियों को भेजता है—अनुरोधकर्ता के सामाजिक नेटवर्क से संपर्क, या शुल्क के बदले काम करने वाले विशेष साक्षी-सेवा प्रदाता।

चरण W2. प्रत्येक साक्षी w_i पूरे हस्ताक्षरित अनुरोध पर हस्ताक्षर करता है, मूल हस्ताक्षर σ_i को रखता है, और एक चुनौती कोड $c_i = h(\sigma_i)$ परिकलित करता है। चुनौती कोड अनुरोध में जोड़ा जाता है।

चरण W3. अब N_w चुनौती कोड ले जाने वाला अनुरोध सत्यापनकर्ता को भेजा जाता है। सत्यापनकर्ता कोडों को देखता है परंतु यह निर्धारित नहीं कर सकता कि साक्षी कौन हैं या क्या कोड वास्तविक हस्ताक्षरों के अनुरूप हैं।

चरण W4 (ईमानदार सत्यापनकर्ता)। यदि सत्यापनकर्ता अपनी घोषित नीति के अनुसार प्रतिक्रिया देता है, तो चुनौती कोड अपारदर्शी बने रहते हैं। साक्षी कभी प्रकट नहीं होते। कोई अतिरिक्त डेटा प्रकाशित नहीं होता।

चरण W5 (नीति उल्लंघन)। यदि सत्यापनकर्ता अपनी नीति का उल्लंघन करता है (अनुरोध की उपेक्षा करता है, असंगत रूप

से प्रतिक्रिया देता है), तो अनुरोधकर्ता के पास साक्षियों के मूल हस्ताक्षर σ_i रहते हैं। इन्हें सहचर डेटा के रूप में प्रकाशित किया जा सकता है: कोई भी $c_i = h(\sigma_i)$ का सत्यापन कर सकता है, जिससे यह सिद्ध होता है कि साक्षी उपस्थित था। अनुरोधकर्ता स्वतंत्र रूप से प्रकाशित कर सकता है—सत्यापनकर्ता ने अपनी प्रतिक्रिया में चुनौती कोडों पर पहले ही हस्ताक्षर कर दिए हैं।

छल गुण। अनुरोधकर्ता कुछ या सभी चुनौती कोडों के स्थान पर यादृच्छिक मान प्रतिस्थापित कर सकता है। सत्यापनकर्ता वास्तविक कोडों (उच्च-प्रतिष्ठा प्राधिकरणों द्वारा समर्थित) को शोर से अलग नहीं पहचान सकता। यह अनिश्चितता ही प्रवर्तन तंत्र है: प्रत्येक अनुरोध इस जोखिम को वहन करता है कि कोई सम्मानित प्राधिकरण गुप्त रूप से निगरानी कर रहा है। इस दबाव को बनाए रखने की लागत लगभग शून्य है (यादृच्छिक संख्याएँ उत्पन्न करना), जबकि सत्यापनकर्ता के लिए बेईमानी की संभावित लागत भयावह है। वास्तविक साक्षियों की अनुपस्थिति में भी ईमानदार व्यवहार को प्रोत्साहित किया जाता है।

साक्षी के रूप में प्राधिकरण। किसी दावे का समर्थन करने वाला प्राधिकरण साक्षी सेवाओं को बंडल कर सकता है: “मैं आपके दावे का समर्थन करता हूँ और सत्यापन के दौरान गुप्त साक्षी के रूप में सेवा देता हूँ।” यह एक स्वाभाविक व्यावसायिक मॉडल है—प्राधिकरण के पास पहले से ही संदर्भ है। तथापि दोनों भूमिकाएँ तार्किक रूप से स्वतंत्र हैं।

5.5 महँगे आमूलवाद का सिद्धांत

तीन लागत चैनल एक साथ संयुक्त होते हैं (चित्र 6):

चैनल 1: पुनरावृत्ति लागत। प्रत्येक अस्वीकृति समय और संसाधन उपभोग करने वाली एक नई पुनरावृत्ति को बाध्य करती है। रैखिक वृद्धि।

चैनल 2: दस्तावेज़ स्फीति। प्रत्येक पुनरावृत्ति पूर्ण सत्यापनकर्ता प्रतिक्रिया को दावा दस्तावेज़ में जोड़ती है। वृद्धि रैखिक है, परंतु आधार ऑफ़सेट के साथ: प्रारंभिक पेलोड (दावा सामग्री, प्राधिकरण समर्थन, क्रिप्टोग्राफिक हस्ताक्षर) का पहले से ही गैर-तुच्छ आकार B_0 होता है। k पुनरावृत्तियों के बाद कुल आकार: $S(k) = B_0 + k \cdot \Delta$, जहाँ Δ औसत प्रतिक्रिया आकार है।

चैनल 3: सत्यापनकर्ता जोखिम प्रीमियम। जोखिम व्यक्तिपरक है। सत्यापनकर्ता आकलन करता है कि क्या अनुरोध करने वाले DID की घोषित नीतियाँ सत्यापनकर्ता के अपने वाणिज्यिक, सामाजिक या राजनीतिक हितों से टकराती हैं। प्रीमियम सत्यापनकर्ता के “आदर्श” से अनुभूत दूरी के साथ चरघातांकी रूप से बढ़ सकता है: $P(d) = \alpha \cdot e^{\beta d}$, जहाँ d सत्यापनकर्ता का व्यक्तिपरक दूरी मापक है। किसी व्यक्तिगत निषिद्ध सीमा के परे, सत्यापनकर्ता पूरी तरह मना कर सकता है।

निर्णायक रूप से, यह सेंसरशिप नहीं है। कोई दावा निषिद्ध नहीं है। व्यवस्था जोखिम की कीमत तय करती है (सारणी 1)।

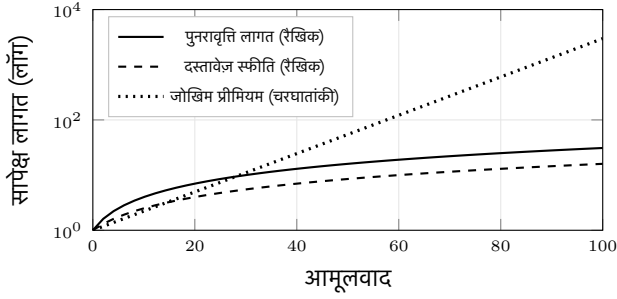


Figure 6: तीन चैनलों में लागत वृद्धि। उच्च आमूलवाद पर जोखिम प्रीमियम प्रभावी हो जाता है।

Table 1: दावा प्रकारों में लागत तुलना।

प्रकार	पुनरा.	दस्ता.	शुल्क	कुल
विश्वसनीय	$k_{\min}$	B_0	$P_{\min}$	निम्न
विवादास्पद	k_{med}	$B_0 + k\Delta$	$\alpha e^{\beta d}$	मध्यम
आमूल	$k_{\max}$	$\gg B_0$	$\gg P_{\min}$	अति उच्च
कपटपूर्ण	$\rightarrow \infty$	—	—	अप्रकाश्य

6 प्रतिष्ठा और जोखिम आकलन

6.1 प्रतिष्ठा संचयन मॉडल

प्रतिष्ठा तीन गुण प्रदर्शित करती है: **धीमा संचयन** (सुसंगत व्यवहार के माध्यम से क्रमिक वृद्धि), **तीव्र विनाश** (एकल कपट अंक को भयावह रूप से घटा सकता है), और **व्यक्तिगत मूल्यांकन** (प्रत्येक उपभोक्ता पक्ष अपना स्वयं का समुच्चयन फलन लागू कर सकता है)।

6.2 प्रतिष्ठित प्राधिकरण

एक प्रतिष्ठित प्राधिकरण दावों की समीक्षा करता है और, संतुष्ट होने पर, उन पर सह-हस्ताक्षर करता है—अपनी स्वयं की प्रतिष्ठा दाँव पर लगाते हुए (चित्र 7)। असममितता जानबूझकर रखी गई है: प्रतिष्ठा अर्जित करना धीमा है (प्रत्येक ईमानदार समर्थन पर क्रमिक $+\delta$), जबकि उसे गँवाना भयावह है (प्रत्येक मिथ्या समर्थन पर $-\Delta \gg \delta$; दृष्टांत के तौर पर, उदा., $+2\%$ बनाम -70%)। इष्टतम रणनीति सदैव संदिग्ध दावों को अस्वीकार करना है। δ और Δ के विशिष्ट मान व्यवस्था के पैरामीटर हैं।

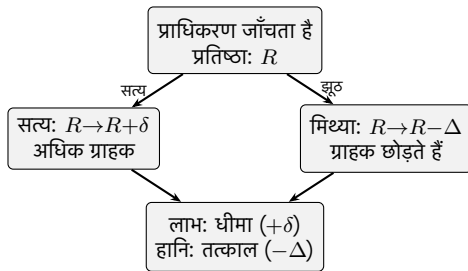


Figure 7: प्रतिष्ठित प्राधिकरण—असममित प्रोत्साहन।

6.3 बहु-आयामी प्रतिष्ठा

प्रतिष्ठा एक अदिश नहीं बल्कि अनेक आयामों में फैला एक सदिश है: वित्तीय विश्वसनीयता, व्यक्तिगत सत्यनिष्ठा, पेशेवर दक्षता, नागरिक सहभागिता, और अन्य (चित्र 8)। विभिन्न मूल्यांकन प्रदाता इस सदिश को संदर्भ के अनुसार भिन्न ढंग से प्रक्षेपित करते हैं—एक ऋणदाता वित्तीय विश्वसनीयता को प्राथमिकता देता है, एक नियोक्ता पेशेवर दक्षता को, एक पड़ोसी नागरिक व्यवहार को। कोई एकल “सही” प्रतिष्ठा अंक नहीं है; केवल दृष्टिकोण हैं।

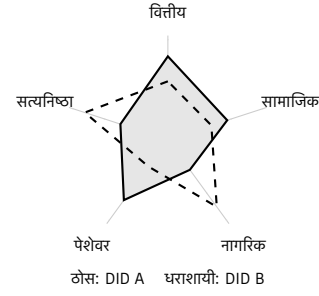


Figure 8: बहु-आयामी प्रतिष्ठा सदिश। विभिन्न DIDs आयामों में भिन्न प्रोफ़ाइल प्रदर्शित करते हैं।

6.4 लोकतांत्रिक जोखिम आकलन

RSN व्यवस्थित जोखिम आकलन का लोकतंत्रीकरण करता है—एक क्षमता जो वर्तमान में वित्तीय संस्थाओं में संकेंद्रित है परंतु बैंकिंग से कहीं आगे तक लागू होती है। आपूर्तिकर्ता विश्वसनीयता का आकलन करने वाले औद्योगिक समूह, व्यवहारगत जोखिम की कीमत तय करने वाली बीमा कंपनियाँ, विलय और अधिग्रहण के लिए यथोचित परिश्रम, विनिर्माण में उपकरण जीवनकाल का अनुमान—जहाँ कहीं भी प्रतिपक्ष जोखिम के आकलन की आवश्यकता होती है, RSN एक विकेंद्रीकृत, बाज़ार-चालित विकल्प प्रदान करता है। व्याख्या सेवाओं का एक बाज़ार कच्चे बहु-आयामी प्रतिष्ठा डेटा को क्रियाशील सारांशों में अनूदित करता है, जिससे प्रतिपक्ष मूल्यांकन किसी भी प्रतिभागी के लिए सीमांत लागत पर सुलभ हो जाता है।

7 सहमति और विवाद समाधान

7.1 विकेंद्रीकृत न्याय मॉडल

RSN न्याय को एक द्विपक्षीय मोलभाव समस्या के रूप में पुनर्परिभाषित करता है। स्थायी, सत्यापन-योग्य प्रतिष्ठा क्षति का खतरा उन कानूनी कार्यवाहियों से अधिक प्रभावी निवारक है जिन्हें पीड़ित पक्ष वहन नहीं कर सकता।

7.2 उदीयमान सहमति

प्रत्येक प्रतिभागी एक व्यक्तिगत संतुष्टि दहलीज़ बनाए रखता है। नेटवर्क की समग्र सहमति हजारों द्विपक्षीय मोलभावों के सांख्यिकीय औसत के रूप में उभरती है (चित्र 9)। सहमति से बहुत ऊपर की प्रतिक्रिया (बर्बर) प्रकाशित करना महंगा है। सहमति के निकट की प्रतिक्रिया (समानुपाती) सस्ती है। सहमति कोई नियम नहीं है—यह एक मूल्य संकेत है।

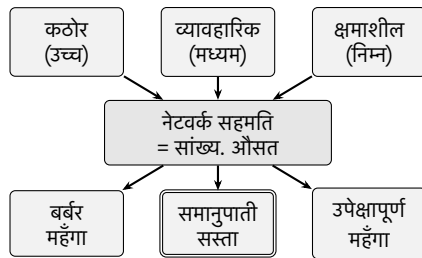


Figure 9: व्यक्तिगत संतुष्टि दहलीज़ों से उदीयमान सहमति।

7.3 दंड अंशांकन

प्रत्येक DID धारक विशिष्ट दुराचार श्रेणियों के प्रति प्रतिक्रियाओं को सार्वजनिक रूप से घोषित करता है। असमानुपातिक रूप से कठोर या उदार घोषणाएँ नकारात्मक प्रतिष्ठा संकेत आकर्षित करती हैं। समानुपाती घोषणाएँ बिना घर्षण के स्वीकार की जाती हैं—एक स्व-अंशांकित दंड व्यवस्था।

सहमति घोषणाएँ स्वयं पाखंड पहचान के अधीन हैं: किसी सहमति स्थिति के प्रति घोषणात्मक रूप से प्रतिबद्ध होते हुए असंगत रूप से व्यवहार करना मूल विचलन से अधिक गंभीर प्रतिष्ठागत अपराध है, क्योंकि यह जानबूझकर किए गए छल को प्रदर्शित करता है।

7.4 प्रत्यायोजन

किसी DID के भीतर की सभी गतिविधियाँ—एक अपवाद के साथ—किसी अन्य DID को प्रत्यायोजित की जा सकती हैं। **विषय भूमिका—वह DID जिसके व्यवहार के बारे में दावा है—प्रत्यायोजित नहीं की जा सकती; यह उस पहचान धारक से अहस्तांतरणीय रूप से बंधी है जिसका दावा उल्लेख करता है।** अन्य सक्रिय भूमिकाएँ—जारीकर्ता, प्राधिकरण, साक्षी, सत्यापनकर्ता—किसी नामित प्रतिनिधि DID को हस्तांतरित की जा सकती हैं, चाहे वह सत्यापन, दावा प्रस्तुति, सहमति भागीदारी, या विवाद समाधान के लिए हो। प्रत्यायोजन किसी भी समय प्रतिसंहरणीय है। यह विशेषीकरण को सक्षम बनाता है (उदा., पेशेवर सत्यापन सेवाएँ) जबकि धारक परम नियंत्रण और उत्तरदायित्व बनाए रखता है। प्रत्यायोजन पूरी व्यवस्था में लागू होता है और मापनीयता के लिए आवश्यक है।

7.5 व्यक्तिगत नैतिकता से उदीयमान सामाजिक अनुबंध तक

प्रत्येक DID की घोषित नीति व्यक्तिगत नैतिकता का औपचारिकीकरण दर्शाती है: धारक क्या स्वीकार्य मानता है, वह विशिष्ट व्यवहारों पर कैसे प्रतिक्रिया देता है, वह प्रतिपक्षों से क्या अपेक्षा करता है। ये नीतियाँ किसी व्यवस्था रचयिता द्वारा थोपी नहीं जाती—इन्हें प्रत्येक प्रतिभागी चुनता है और मशीन-पठनीय रूप में व्यक्त करता है।

यह औपचारिकीकरण एक त्रि-चरणीय उद्भव को सक्षम बनाता है। पहला, व्यक्तिगत नैतिकता **नीति** के रूप में संकेतित होती है—घोषित नियमों, दहलीज़ों, और प्रतिक्रिया फलनों का एक समुच्चय जिसका पालन करने के लिए DID प्रतिबद्ध होता है। दूसरा, नेटवर्क भर की सभी नीतियों का समुच्चय **उदीयमान नैतिकता** उत्पन्न करता है—सांख्यिकीय रूप से प्रेक्षणीय मानदंड जिन्हें किसी एकल प्रतिभागी ने नहीं गढ़ा परंतु जो हजारों व्यक्तिगत नैतिक स्थितियों की अंतःक्रिया से उत्पन्न होते हैं [9]। तीसरा, ये उदीयमान नैतिकताएँ, द्विपक्षीय मूल्य संकेतों के माध्यम से प्रवर्तित साझा व्यवहारगत मानदंडों के रूप में व्यक्त, एक **मापन-योग्य सामाजिक अनुबंध** का गठन करती हैं—कोई सैद्धांतिक निर्मिति नहीं जिस पर किसी ने हस्ताक्षर नहीं किए [10], बल्कि वास्तविक व्यवहार से समर्थित एक अनुभवजन्य रूप से प्रेक्षणीय नियम-समुच्चय।

यह प्रक्रिया नैतिक आधार सिद्धांत के निष्कर्षों को प्रतिबिंबित करती है [11]: मानव नैतिकता सहज, बहुलवादी, और सांस्कृतिक रूप से परिवर्तनशील है। RSN को इनपुट के रूप में नैतिक सहमति की आवश्यकता नहीं है; यह आउटपुट के रूप में व्यवहारगत सहमति उत्पन्न करता है। परिणामी सामाजिक अनुबंध स्थिर नहीं है—यह तब विकसित होता है जब प्रतिभागी जुड़ते हैं, छोड़ते हैं, और नेटवर्क फीडबैक के जवाब में अपनी नीतियों को समायोजित करते हैं। शास्त्रीय सामाजिक अनुबंध सिद्धांत के विपरीत, यह अनुबंध प्रतिसंहरणीय, प्रेक्षणीय, और बिना किसी संप्रभु के प्रवर्तनीय है।

8 आर्थिक मॉडल

पूर्ववर्ती खंडों में एक उपकरण का वर्णन किया गया—RSN के सत्यापन तंत्र, लागत संरचना, और उदीयमान सहमति। यह खंड इस उपकरण को राजकोषीय और शासन संक्रमण पर लागू करने की एक कार्यप्रणाली का वर्णन करता है। उपकरण सामान्य-प्रयोजन का है; नीचे दी गई कार्यप्रणाली एक संभावित अनुप्रयोग है।

8.1 प्रोत्साहन संरचना

पूँजी के रूप में प्रतिष्ठा ईमानदार व्यवहार के लिए प्रत्यक्ष प्रोत्साहन उत्पन्न करती है। सामान्य संचालन में, प्रतिभागी रोजमर्रा के लेनदेन और पूर्ण की गई प्रतिबद्धताओं के माध्यम से स्वाभाविक रूप से प्रतिष्ठा बनाते हैं। प्राथमिक व्यय नकारात्मक दावों पर होता है—दूसरों द्वारा की गई हानि को दर्ज करना। यह असममितता उपयोगी, विश्वसनीय व्यवहार को प्रोत्साहित करती

है: ईमानदार होने पर कोई अतिरिक्त लागत नहीं आती, जबकि हानिकारक होने पर एक प्रलेखित निशान बनता है जिसे दूसरे संरक्षित करने के लिए भुगतान करेंगे। पाखंड—नियमों की घोषणा किए बिना उनका पालन करना—सबसे महंगा विफलता तरीका है, क्योंकि यह जानबूझकर किए गए छल को प्रदर्शित करता है।

8.2 समानांतर राजकोषीय व्यवस्था

तीन घटक प्रतिस्पर्धात्मक दबाव को सक्षम बनाते हैं: (1) **सरल कर**—बिना किसी अपवाद के एकल समानुपाती दर, प्रारंभ में मौजूदा प्रभावी दर से मामूली रूप से नीचे; (2) **इलेक्ट्रॉनिक व्यय पंजीकरण (ESR)**—चेक EET मॉडल का उलटाव ताकि नागरिक राज्य के व्ययों की निगरानी करें; (3) **नागरिक-निर्देशित कर आवंटन**—पहले वर्ष में कुछ प्रतिशत से शुरू होकर, एक दशक बाद, अपनाव की दर के आधार पर, निम्न दो-अंकीय आँकड़ों से लेकर पूर्ण नागरिक-निर्देशित व्यवस्था तक कहीं भी पहुँचना। वास्तविक गति उस गति पर निर्भर करती है जिससे राज्य सेवाओं के मुक्त-बाजार विकल्प उभरते हैं और संक्रमण में सहयोग करने की राज्य की इच्छा पर; समय का फलन रैखिक होना आवश्यक नहीं है, और अपनाव अंततः कहाँ पहुँच सकता है इस पर ऊपरी सीमा निर्धारित करने का कोई कारण नहीं है।

9 स्थानांतरण मार्ग

स्थानांतरण तीन चरणों से होकर बढ़ता है (चित्र 10): **चरण 1: अध्यारोपण** (सूचनात्मक परत के रूप में RSN, राज्य एकमात्र प्रदाता), **चरण 2: प्रतिस्पर्धा** (RSN कार्यात्मक विकल्प प्रदान करता है, द्वैध-व्यवस्था उपयोग), और **चरण 3: संक्रमण** (RSN राज्य के समकक्षों से बेहतर प्रदर्शन करता है, स्वैच्छिक स्थानांतरण)। संक्रमण हर चरण पर प्रतिवर्ती है।

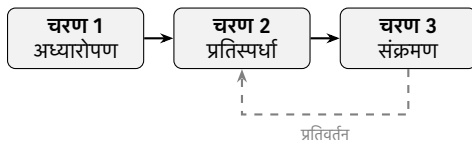


Figure 10: तीन-चरणीय स्थानांतरण—हर चरण पर प्रतिवर्ती।

प्राथमिक दबाव तंत्र राजकोषीय है: जब सशर्त करदाता एक “आर्थिक रूप से महत्वपूर्ण अल्पसंख्या X ” तक पहुँचते हैं—एक ऐसा समूह जो इतना बड़ा हो कि उसके विरुद्ध दमन गैर-तुच्छ आर्थिक क्षति पहुँचाए और नागरिक अवज्ञा एक विश्वसनीय खतरा बन जाए—तब राज्य वार्ता में प्रवेश करता है। दृष्टान्त के लिए, हम $X \approx 15\%$ GDP का उपयोग करते हैं, परंतु वास्तविक दहलीज़ विशिष्ट अर्थव्यवस्था पर निर्भर करती है।

10 सुरक्षा विश्लेषण

हम पाँच प्रतिकूल श्रेणियों पर विचार करते हैं: व्यक्तिगत दुष्ट अभिकर्ता, संगठित समूह, कॉर्पोरेट प्रतिकूल, राज्य-स्तरीय

प्रतिकूल, और प्रोटोकॉल-स्तरीय प्रतिकूल।

सिबिल प्रतिरोध [12]। प्रतिष्ठा बनाने के लिए सतत, सत्यापन-योग्य अंतःक्रिया आवश्यक है। एक सफल सिबिल हमले की लागत नकली पहचानों के साथ रैखिक रूप से और लक्ष्य प्रतिष्ठा स्तर के साथ द्विघातीय रूप से बढ़ती है। समानांतर में अनेक DIDs संचालित करना संभव है परंतु डिज़ाइन से महंगा है—प्रत्येक पहचान को वास्तविक गतिविधि के माध्यम से स्वतंत्र रूप से प्रतिष्ठा संचित करनी होती है। स्वतंत्र समाजों में यह लागत अनौपचारिक दुरुपयोग को रोकती है; तानाशाहियों में, समानांतर DIDs एक उत्तरजीविता उपकरण बन जाते हैं जो खंडीकृत प्रतिरोध, भूमिगत समन्वय, और सुरक्षित काला-बाज़ार संचालन को सक्षम बनाते हैं।

सांठांठ बचाव। बंद समूहों के बीच पारस्परिक समर्थन के पैटर्न सामाजिक आलेख विश्लेषण के माध्यम से पहचाने जाने योग्य हैं। प्रतिष्ठा समुच्चयन फलन घनिष्ठ रूप से गुच्छित स्रोतों से आने वाले दावों को छूट देते हैं।

राज्य-स्तरीय प्रतिकूल। ओनियन रूटिंग, केंद्रीकृत अवसंरचना की अनुपस्थिति, और सत्यापनकर्ता भूमिका का प्रतिभागी आधार में वितरण यह सुनिश्चित करते हैं कि दमन के लिए किसी भी लाभ की तुलना में असमानुपातिक उपाय आवश्यक होते हैं।

गोपनीयता बनाम जवाबदेही। छद्मनामिता—गुमनामी और पहचान प्रकटीकरण के बीच का एक मध्यमार्ग—DIDs को धारक की वास्तविक-जगत पहचान प्रकट किए बिना सार्थक प्रतिष्ठा संचित करने की अनुमति देती है।

11 गोपनीयता संबंधी विचार

RSN का गोपनीयता मॉडल छद्मनामिता पर निर्मित है। धारक पहचान प्रकटीकरण को नियंत्रित करता है: न्यूनतम (शुद्ध छद्मनाम), चयनात्मक (विशिष्ट प्रमाणपत्र जुड़े हुए), या पूर्ण (कानूनी पहचान संबद्ध)। प्रकाशित दावे स्थायी होते हैं—व्यवस्था संदर्भगत सुधार का समर्थन करती है परंतु विलोपन का नहीं। एक धारक किसी समझौता की गई DID को त्यागकर नए सिरे से शुरू कर सकता है, संचित प्रतिष्ठा को गँवाते हुए।

12 संबंधित कार्य

W3C DID Core विशिष्टि [2] और Ceramic Network [8] पहचान आधार प्रदान करते हैं। EigenTrust [13] ने बिना केंद्रीय प्राधिकरण के वितरित प्रतिष्ठा समुच्चयन को प्रदर्शित किया। SBTs [3] ने अहस्तांतरणीय सामाजिक टोकन प्रस्तुत किए। RSN गुणवत्ता फ़िल्टर के रूप में आर्थिक लागत पर अपने बल और आमूलवाद की कीमत तय करने के अपने तंत्र में भिन्न है।

DAOs [4] और द्विघातीय मतदान [5] ने विकेंद्रीकृत शासन की व्यवहार्यता को प्रदर्शित किया। RSN सहमति को मतदान के बजाय द्विपक्षीय मूल्य वार्ताओं से व्युत्पन्न करता है।

यह प्रस्ताव निजी सेवा प्रावधान के लिए अराजक-पूँजीवादी

सिद्धांत [14, 15] पर आधारित है परंतु दो निर्णायक पहलुओं में विचलित होता है: यह तर्कसंगतता मानने के बजाय द्वेष और प्रतिशोधात्मक आवेगों के लिए डिजाइन करता है, और यह क्रांति के बजाय क्रमिक संक्रमण का प्रस्ताव करता है। उदीयमान सामाजिक अनुबंधों की अवधारणा के पूर्ववर्ती हायेक के स्वतःस्फूर्त व्यवस्था के सिद्धांत [16] में हैं।

अराजक-एगोरिज्म। RSN एगोरिस्ट प्रति-अर्थशास्त्र [17] के साथ महत्वपूर्ण साझा आधार साझा करता है—विशेष रूप से समानांतर संस्थाओं के निर्माण और स्वैच्छिक विनिमय पर बल। तथापि, एगोरिज्म तर्कसंगत स्वार्थ को एक पर्याप्त समन्वय तंत्र मानने की प्रवृत्ति रखता है और अक्सर मौजूदा राज्य संरचनाओं से एक ठोस स्थानांतरण मार्ग का अभाव रखता है। RSN स्पष्ट रूप से गैर-तर्कसंगत व्यवहारगत प्रवृत्तियों को समाहित करता है और क्रमिक संक्रमण के लिए एक राजकोषीय दबाव तंत्र प्रदान करता है।

योग्यतातंत्र। RSN संभवतः इस बात का पहला कार्यात्मक वर्णन दर्शाता है कि योग्यतातंत्र [18] एक नारे के बजाय एक तांत्रिक गुण के रूप में कैसे उभर सकता है। पारंपरिक योग्यतातांत्रिक व्यवस्थाएँ इसलिए विफल होती हैं क्योंकि उन्हें “योग्यता” को परिभाषित और प्रवर्तित करने के लिए एक केंद्रीय प्राधिकरण की आवश्यकता होती है। RSN में, योग्यता द्विपक्षीय मूल्यांकनों से उभरती है: जो मूल्य प्रदान करते हैं वे प्रतिष्ठा संचित करते हैं; कोई समिति यह तय नहीं करती कि किसमें योग्यता है।

विशेषाधिकार के रूप में संपत्ति। RSN संपत्ति अधिकारों को प्राकृतिक और निरपेक्ष मानने वाले अराजक-पूँजीवादी और ऑस्ट्रियन-स्कूल के दृष्टिकोणों से मौलिक रूप से विचलित होता है। RSN ढाँचे में, संपत्ति एक विशेषाधिकार है—एक सामाजिक मान्यता जिसे, चरम मामलों में, समुदाय द्वारा तब वापस लिया जा सकता है जब कोई प्रतिभागी साझा मानदंडों का मौलिक रूप से उल्लंघन करता है (विश्वासघात, अस्तित्वगत संकट में समुदाय की रक्षा करने से इनकार, व्यवस्थित शोषण)। यह राज्य द्वारा अधिग्रहण नहीं बल्कि द्विपक्षीय संबंधों के नेटवर्क द्वारा सामाजिक मान्यता का प्रत्याहरण है।

13 चर्चा और सीमाएँ

ठंडी शुरुआत। RSN का मूल्य नेटवर्क प्रभावों पर निर्भर करता है; प्रारंभिक अपनाने वाले तब तक सीमित मूल्य का सामना करते हैं जब तक भागीदारी एक दहलीज़ तक नहीं पहुँच जाती। तथापि, प्रारंभिक चरणों से भी, DID नेटवर्क एक उपयोगी पूरक सूचना स्रोत के रूप में काम करता है। प्रारंभिक प्रतिष्ठा मूल्यांकन और प्राधिकरण आकलन के बढ़ती परिष्कृतता के साथ क्रमशः विकसित होने की अपेक्षा है।

एंटी-लीचिंग और पहुँच नियंत्रण। लक्ष्य DIDs कम-प्रतिष्ठा वाले DIDs से आने वाले प्रश्नों पर क्रमिक शुल्क और पहुँच प्रतिबंध लगा सकते हैं। यह द्विआधारी नहीं बल्कि एक सतत पैमाना है: प्रश्न करने वाले DID के पास जितनी कम प्रतिष्ठा होती है, उसे उतनी ही कम सूचना मिलती है, उतना ही अधिक प्रतीक्षा करता है, और उतना ही अधिक भुगतान करता है। यह तंत्र निष्क्रिय उपभोग के बजाय वास्तविक भागीदारी को प्रोत्साहित करता है।

पहुँच की असमानता। दावे प्रकाशित करने की लागत आर्थिक रूप से वंचित प्रतिभागियों की वैध शिकायतों को छाँट सकती है। शमन: प्रत्येक प्रतिभागी एक साथ एक संभावित सत्यापनकर्ता के रूप में काम करता है (या इस भूमिका को प्रत्यायोजित करता है) और सत्यापन शुल्क अर्जित करता है। पर्याप्त समयावधि में, एक गैर-आमूल प्रतिभागी को वित्तीय तटस्थता के करीब पहुँचना चाहिए—सत्यापन आय लगभग प्रकाशन लागतों की भरपाई करती है। यह एक सांख्यिकीय अपेक्षा है, गारंटी नहीं।

प्रतिष्ठा असमानता। प्रारंभिक अपनाने वाले ऐसे लाभ संचित करते हैं जो बाद में आने वालों के लिए बाधाएँ पैदा कर सकते हैं। तथापि, प्रतिष्ठा मूल्यांकन तृतीय-पक्ष प्रदाताओं द्वारा किया जाता है जो अपने समुच्चयन एल्गोरिदम के माध्यम से प्रथम-प्रवर्तक लाभ को कम करना चुन सकते हैं। अच्छी प्रतिष्ठा के साथ पहला होना एक वैध तुलनात्मक आर्थिक लाभ है—और यह डिजाइन से है।

खुले प्रश्न। इष्टतम लागत फलन, समुच्चयन मानक, प्रोटोकॉल शासन, और AI-जनित कृत्रिम प्रतिष्ठा डेटा के साथ अंतःक्रिया भविष्य के कार्य के क्षेत्र बने हुए हैं।

यह शोधपत्र यह दावा नहीं करता कि RSN सभी परिस्थितियों में इष्टतम परिणाम उत्पन्न करेगा। यह दावा करता है कि RSN एक व्यवहार्य विकल्प दर्शाता है—तकनीकी रूप से क्रियान्वयन-योग्य, आर्थिक रूप से स्व-टिकाऊ, और मानवीय व्यवहारगत प्रवृत्तियों के साथ सामाजिक रूप से संगत जैसी वे वास्तव में हैं।

14 निष्कर्ष

इस शोधपत्र ने प्रतिष्ठा सामाजिक नेटवर्क प्रस्तुत किया है, एक विकेंद्रीकृत प्रोटोकॉल जो छद्मनामी, सत्यापन-योग्य प्रतिष्ठा विनिमय को सक्षम बनाता है। मंहेंगे आमूलवाद का सिद्धांत यह सुनिश्चित करता है कि कपटपूर्ण दावे बिना सेंसरशिप के मूल्य के आधार पर बाहर हो जाएँ। प्रस्तावित स्थानांतरण मार्ग मौजूदा संस्थाओं से क्रमिक, प्रतिवर्ती संक्रमण को सक्षम बनाता है। यह डिजाइन मानव प्रकृति को वैसे ही समाहित करता है जैसी वह है—क्षुद्रता, द्वेष, और प्रतिशोधात्मक संतुष्टि की इच्छा सहित—न कि वैचारिक रूपांतरण की माँग करते हुए। परिणाम यूटोपिया नहीं बल्कि एक ऐसी व्यवस्था है जहाँ न्याय सुलभ है, प्रतिष्ठा अर्जित की जाती है, और दुराचार की लागत उस पक्ष द्वारा वहन की जाती है जिसने उसे उत्पन्न किया।

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.