

Merkeziyetsiz İtibar Ağı: Doğal Toplumsal Örgütlenme İçin Bir Çerçeve

Pavel Kudrna
Prague, Czechia
Draft v1 — March 2026

Abstract

Adalet duygusu—haksızlıkların düzeltildiği ve liyakatin ödüllendirildiği inancı—toplumun en güçlü birleştirici gücüdür. Bir hakkı uygulamanın maliyeti hakkın kendisinin değerini aştığı için merkezî yönetim kurumları bu duyguyu sağlayamadığında, toplumsal uyum aşınır. Mevcut kurumsal yapılar, önemli bir uyuşmazlık sınıfını, merkezî planlamanın kaynakları tahsis etmekte başarısız olmasıyla sistematik olarak aynı biçimde çözmekte başarısız olur: bilgi asimetrisi, eksik geri bildirim döngüleri ve karar vericilerin kararlarının sonuçlarından kopukluğu yoluyla. Bu makale bir İtibar Sosyal Ağı (RSN) sunar: Merkeziyetsiz Kimlik Belirteçleri (DID) üzerine kurulu, takma adlı katılımcıların gerçek dünyadaki davranışlar hakkındaki itibar bilgilerini yayımlamasını, doğrulamasını ve tüketmesini sağlayan merkeziyetsiz, yozlaştırılmaz, sansüre dirençli bir iletişim katmanı. Temel mekanizma üç tasarım ilkesine dayanır: (1) itibar verilerini okumanın ucuz olduğu ancak yazmanın doğrulanabilir çaba gerektirdiği asimetrik bir maliyet yapısı; (2) radikal iddiaları giderek artan yineleme maliyetleri aracılığıyla fiyatlandıran, tutarlı özetlemeye (consistent hashing) dayalı deterministik olmayan bir doğrulayıcı seçim protokolü; ve (3) özel doğrulayıcıların onayladıkları iddiaların doğruluğuna biriktirdikleri itibarı ortaya koydukları, piyasa güdümlü bir itibar otoritesi modeli. Ortaya çıkan mimari, merkezî koordinasyon olmaksızın kendiliğinden bir liyakat sistemi üretir ve mevcut devlet tarafından yönetilen sistemlerden kademeli, geri döndürülebilir bir geçiş yolu sağlar.

1 Giriş

1.1 Merkezî Güvenin Sorunu

Modern yönetim temel bir varsayıma dayanır: merkezî kurumların, yabancılar arasındaki güveni ölçekte aracılık edebileceği. Mahkemeler uyuşmazlıkları

çözer. Siciller mülkiyeti belgeler. Düzenleyici kurumlar standartları uygular. Bu kurumlar, bilginin kıt olduğu, iletişimin yavaş olduğu ve yetkinin merkezî bir organa devredilmesinin tek uygulanabilir koordinasyon mekanizması olduğu bir çağda tasarlanmıştı. Ancak merkezî yönetim, merkezî planlamayla aynı yapısal nedenlerle başarısız olur: bilgi asimetrisi, eksik geri bildirim döngüleri ve karar vericilerin kararlarının sonuçlarından kopukluğu.

Bu varsayım, örneğin kurumsal aracılığın maliyeti uyuşmazlığın değerini aştığında başarısız olur. Kiraladığı dairenin yasal olarak zorunlu bir elektrik güvenliği belgesinden yoksun olduğunu keşfeden bir kiracıyı düşünün—hayat için doğrudan tehlike oluşturan bir durum. Kiracının sözleşmeden çekilme yönündeki yasal hakkı tartışmasızdır. Ancak bu hakkı mahkeme sistemi aracılığıyla uygulamanın maliyeti, potansiyel yasal tazminat dahil olmak üzere, depozitonun ve alacaklı olunan zararların parasal değerini aşar [1]. Rasyonel yanıt, kaybı üstlenmek ve çıkmaktır.

Bu, patolojik bir uç durum değildir. Zararın gerçek olduğu ancak parasal riskin, kurumsal uygulamanın ekonomik olarak rasyonel hale geldiği eşğin altına düştüğü önemli bir uyuşmazlık sınıfı için varsayılan deneyimdir. Sonuç, kötü niyetli aktörleri yapısal olarak kayıran bir sistemdir: başkalarına bu eşğin altındaki hacimlerde zarar verenler cezasız kalabilir, çünkü adalet arama maliyeti zarar gören tarafa düşer.

Yukarıdaki örnek, yazarın hukukî ortamından—Çek medenî hukuk sisteminden—alınmıştır. Diğer hukuk geleneklerinde—içtihat temelli ortak hukuk (common law), örf ve âdet hukuku, karma sistemler—adalet, yargı çevresinin kültürel ve usulî özelliklerine bağlı olarak farklı biçimlerde ve farklı derecelerde başarısız olur. Okurlar muhtemelen kendi bağlamlarından eşdeğer örnekler tanıyacaklardır. Yapısal olarak evrensel olan örüntüdür: değeri ekonomik olarak rasyonel uygulama eşğinin altına düşen uyuşmazlıklar, kaybın zarar gören tarafça üstlenilmesiyle son bulur. RSN mükemmel adalet vaat etmez—yalnızca kurumsal uygulamanın ekonomik olmadığı

durumlarda kötü niyetli aktörlerin sahip olduğu yapısal avantajı azaltır.

1.2 Mevcut Çözümler Neden Yetersiz Kalıyor

Merkeziyetsiz Kimlik (DID) çerçeveleri [2] özgeçim kimlik yönetimi için kriptografik mekanizmalar sağlar ancak öncelikle kimlik doğrulamaya odaklanır ve davranışsal itibarın daha geniş sorununu ele almaz.

Ruha Bağlı Belirteçler (SBT'ler) [3] itibarın devredilemez olduğu içgörüsünü yakalar ancak ölçeklenebilirlik kısıtlamaları olan blok zinciri altyapısına dayanır ve bilgi girişini yöneten ekonomik teşvikleri ele almaz. Liyakat belirteçleri (ör. Liberland) gibi ilgili kavramlar benzer bir felsefeyi paylaşır ancak belirli yargı çerçevelerine bağlı kalır.

Merkeziyetsiz Özerk Organizasyonlar (DAO'lar) [4] yönetimi akıllı sözleşmeler aracılığıyla uygular ancak etkinin sermayeyle orantılı olduğu plütokratik dinamikleri yeniden üretir. Karesel oylama [5] bunu kısmen hafifletir ancak pratik benimsemeyi sınırlar. DAO'lar ayrıca temel *kâhin* (*oracle*) *sorunuyla* karşı karşıyadır: akıllı sözleşmeler güvenilir bir dış kaynak olmadan gerçek dünya durumlarını güvenilir biçimde doğrulayamaz ve bu sorunun blok zinciri mimarisi içinde genel bir çözümü yoktur.

Mevcut hiçbir sistem merkeziyetsizliği, sansür direncini, takma adlılığı, doğrulanabilir giriş maliyetini ve kendiliğinden oluşan uzlaşmayı bir arada barındırmaz.

1.3 Katkılar

Bu makale şu katkıları sunar:

1. DID çerçevesini iki yönlü itibar değişimini destekleyecek şekilde genişleten merkeziyetsiz bir protokol olan **İtibar Sosyal Ağı'nın (RSN)** tanımı.
2. Tutarlı özetlemeye dayalı **deterministik olmayan bir doğrulayıcı seçim protokolü** [6].
3. İddiaları, üç bileşik maliyet kanalı aracılığıyla ağ uzlaşısından uzaklıklarına göre fiyatlandıran **Pahalı Radikalite İlkesi**.
4. Sahte onayın maliyetinin meşru ücretlerden felaket derecesinde daha fazla olduğu, asimetrik teşviklere sahip bir **İtibarlı Otorite modeli**.
5. Paralel malî altyapı aracılığıyla **kademeli bir geçiş yolu**.

2 Tasarım İlkeleri

RSN mimarisi, pazarlığa açık olmayan beş tasarım ilkesiyle kısıtlanmıştır.

Süreklilik ve Evrim. Sistem, belirsiz uzunlukta bir geçiş döneminde mevcut kurumlarla bir arada var olur. Geçiş her aşamada geri döndürülebilir olmalıdır.

Gönüllülük ve Sorumluluk. Katılım gönüllüdür ancak gönüllülük sorumlulukla eşleşir: kurumsal bir işlev üzerinde denetim üstlenen bir katılımcı, eşzamanlı olarak beraberindeki yükümlülükleri de üstlenir.

Çeşitlilik ve Kültürel Tarafsızlık. Uzlaş, sistem tasarımcıları tarafından dayatılan önceden belirlenmiş kurallardan değil, iki yönlü etkileşimlerden ortaya çıkar.

Dayanıklılık ve Sansür Direnci. Ağ sansürlemenin maliyeti, ona katlanmanın maliyetini aşmalıdır. Sistemi yalnızca tam totaliterlik—yıkıcı siyasî ve ekonomik maliyetle—bastırabilir.

Uzlaş ve Uygulama. Sistem, insanın küçüklük, kin ve intikam alma tatminine yönelik eğilimlerini taşıyıcı özellikler olarak bünyesine katar. Kötü davranış yasaklanmaz; fiyatlandırılır.

3 Sisteme Genel Bakış

3.1 İtibar Sosyal Ağı

RSN, katılımcıların gerçek dünyadaki davranışlar hakkında doğrulanabilir bilgi alışverişinde bulunduğu merkeziyetsiz, uçtan uca (peer-to-peer) bir iletişim katmanıdır. Tanımlayıcı özellikleri şunlardır: merkeziyetsiz ve sansürlenemez altyapı; DID'ler aracılığıyla takma adlı katılım; asimetrik maliyet yapısı (okumak ucuz, yazmak pahalıdır); kriptografik doğrulanabilirlik; ve **standart desteği**—ağ üzerinden yayılan bilgiler için, otoriteler tarafından sunulan hizmetler için (iddia oluşturma, onaylama, tanık hizmeti) ve karşı taraf itibarını değerlendirme kurallarını ve politika uyumsuzluğu riskini (beyan edilen ile fiilî davranış arasında) değerlendirmeyi içeren politika biçimi için makinece okunabilir formatlar.

3.2 Mimarî Bileşenler

RSN dört ana bileşenden oluşur (Şek. 1):

1. **DID Katmanı.** Beyan edilen kurallar, itibar meta verileri ve ağ yönlendirmesi ile katılımcı kimlikleri.
2. **İddia Protokolü.** Gerçek dünya olayları hakkındaki iddiaları yayımlamak için yapılandırılmış

format.

3. **Doğrulama Ağı.** Tutarlı özetleme kullanarak doğrulayıcı atamaya yönelik merkeziyetsiz protokol.
4. **İtibar Toplama Katmanı.** İnsan tarafından okunabilir itibar özetleri üreten hizmetler.

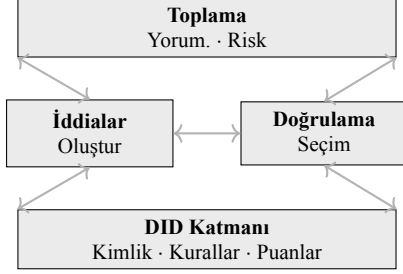


Figure 1: RSN dört katmanlı mimarisi.

3.3 Katılımcı Roller

Bir doğrulama işlemi en fazla altı farklı DID rolünü içerir (Şek. 2): **İhraççı** (DID_I , iddiayı oluşturur ve sunar), **Özne** (DID_S , iddianın hakkında olduğu DID—İhraççı ile örtüşebilir), **Otorite** (DID_A , iddiayı bir ücret karşılığında onaylar; tanık hizmetleri de sunabilir—*isteğe bağlı*), **Tanık** ($DID_{W1..n}$, meydan okuma kodları aracılığıyla doğrulayıcı dürüstlüğü gizlice izleyen—*isteğe bağlı*), **Doğrulayıcı** (DID_V , iddiayı yayımlamak üzere algoritmik olarak seçilen) ve **RSN** (doğrulanmış iddiaların yayımlandığı ağ). Herhangi bir rol başka bir DID'e devredilebilir (Bölüm 7.4). Bir Otorite genellikle onaylamayı tanık hizmetleriyle birleştirir ancak bu iki işlev mantıksal olarak bağımsızdır.

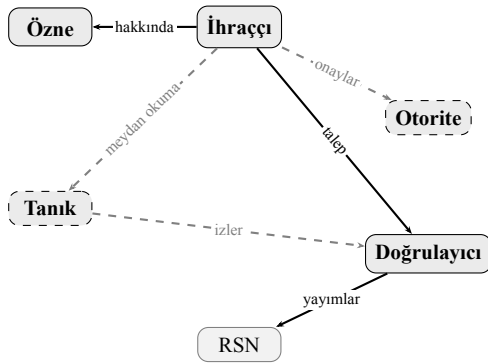


Figure 2: Bir doğrulama işlemindeki DID rolleri. Kesikli = isteğe bağlı (Otorite, Tanık).

3.4 Yozlaştırılmazlık: Dört Güç

RSN'nin yozlaştırılmazlığı tek bir mekanizmadan değil, eşzamanlı dört güçten kaynaklanır. Hiçbiri tek

başına yeterli değildir; yalnızca bunların birleşimi yozlaştırma girişimini ekonomik olarak akıl dışı kılar.

Öngörülemez hedef. Her iddia için doğrulayıcı, tutarlı özetleme yoluyla deterministik olmayan biçimde seçilir (Bölüm 5.3). Bir saldırgan rüşvet için belirli bir doğrulayıcıyı önceden hedefleyemez, çünkü doğrulayıcının kimliği ihraççının seçiminin değil, iddianın içeriğinin ve önceki yinelemelerin bir işlevidir.

İtibar kaldırıcı—yavaş yükselir, hızlı düşer. İtibar yalnızca kademeli olarak, sürekli tutarlı davranışla kazanılabilir. Ancak tek bir sahtekârca onayda felaket derecesinde kaybedilebilir (Bölüm 6.2). Bu asimetri, yıllarca biriktirilen itibarın tek bir sahtekârca onayla yok edilebileceği anlamına gelir; optimal strateji şüpheli iddiaları reddetmek olarak kalır.

Kamusal vaat. Her DID Sahibi kendi politikasını—uymayı taahhüt ettiği makinece okunabilir bir kurallar dizisini—kamuya açık olarak beyan eder. Beyan ile fiilî davranış arasındaki ayrışma tespit edilebilir ve temeldeki ihlalden daha ağır bir itibar suçu olarak fiyatlandırılır (Bölüm 7.3). Bu nedenle ikiyüzlülük, doğrudan sahtekârlıktan daha maliyetlidir.

Örgü ağı saldırı-maliyet asimetrisi. Ağı sansürleme veya istikrarsızlaştırma maliyeti ağın büyüklüğü ve yoğunluğuyla doğrusal olmayan biçimde artarken, ona katlanma maliyeti sabit kalır. Sansürün getiri sağlaması için merkezî bir aktörün bunu ağına tamamına uygulaması gerekir—düşünülebilecek herhangi bir yararla orantısız önlemler gerektirir (Bölüm 10).

4 Merkeziyetsiz Kimlik Modeli

4.1 Özel Özelliklere Sahip DID

RSN, W3C DID Core spesifikasyonunu [2] şu unsurlarla genişletir: **Beyan Edilen Kurallar** (makinece okunabilir davranışsal taahhütler), **İtibar Meta Verileri** (toplu davranışsal puan) ve **Ağ Yönlendirmesi** (kararlı halka konumundan ayrı, değiştirilebilir soğan geçidi).

4.2 İddia Yaşam Döngüsü

Bir İddia altı aşamadan geçer (Şek. 3): oluşturma, isteğe bağlı otorite onayı, tutarlı özetleme yoluyla doğrulayıcı seçimi, doğrulama kararı (kabul veya yinelemeyle ret), yayımlama ve tüm taraflar için itibar güncellemesi.

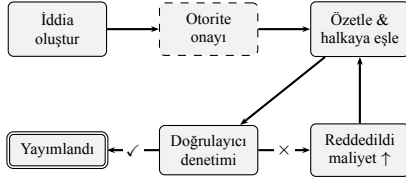


Figure 3: Yineleme döngülü iddia yaşam döngüsü.

4.3 W3C DID Core ile İlişki

RSN'nin kimlik modeli, W3C DID Core spesifikasyonunun [2] tam bir üst kümesidir. Tüm RSN DID'leri geçerli W3C DID'leridir. RSN'ye özgü genişletmeler, ION [7] ve Ceramic [8] gibi mevcut altyapılarla uyumlu, özel bir DID yöntemi spesifikasyonunda tanımlanan DID belgesi özellikleri olarak kodlanır.

5 Bilginin Doğrulanması ve Yayılması

5.1 Bilgi Girişinin Maliyeti

RSN'nin temel ekonomik ilkesi, okuma ile yazma arasındaki asimetridir. İtibar verilerini okumak, DID ağının parçası olan ve itibarlarıyla orantılı erişime sahip katılımcılar için sıfır marjinal maliyete yaklaşır—yeni katılanlar daha geniş erişimi kademeli olarak hak etmelidir (bkz. asalaklığı önleme). Yazmak—tek seferlik bir teknik eylem olarak değil, itibarın ağa kalıcı biçimde maddeleşmesi olarak anlaşılan—üç boyutta doğrulanabilir birikimli yatırım gerektirir: **zaman** (tutarlı davranışa, yerine getirilen taahhütlere ve geliştirilen ilişkilere harcanan yıllar), **enerji** (dürüst ilişkilere, ortaklıklara özene ve uzun vadeli güvenilirliğe yatırılan çaba) ve **para** (kişinin kendi adına yatırımı—mesleki gelişim, işinin kalitesi, verilen zararların telafisi). İtibar anında satın alınmaz—sistemin yalnızca görünür ve bağlamlar arasında aktarılabilir kıldığı, yaşam boyu süren bir birikimin sonucudur. Protokolün tek seferlik teknik maliyetleri (kriptografik imzalar, doğrulayıcı ücretleri) bu temel yatırıma kıyasla ihmal edilebilir düzeydedir.

5.2 Sosyal Grafik ve Bağlantı Derinliği

RSN temelde bir sosyal ağıdır: her DID, bağlantıya izin veren kişileri (diğer DID'leri) ekler. Bu bağlantıların kendi bağlantıları vardır ve bu böyle devam eder. Algoritmik doğrulayıcı araması, yapılandırılabilir bir h derinliğindeki bağlı kişiler içinde çalışır (ör. $h = 3$: kişinin doğrudan bağlantıları, onların bağlantıları ve bağlantıların bağlantıları). Bu mimari tek

bir küresel blok zinciri gerektirmez—diğer topluluklara örtüşmeler içeren toplulukların/kümelerin ortaya çıkmasını doğal olarak destekler. Her DID katılımcısının yayımlanmış bir **politikası**—gelen taleplerin nasıl değerlendirileceğini yöneten makinece okunabilir bir kurallar dizisi—olmalıdır. Politika ihlalleri ağda olumsuz eserler olarak kaydedilir.

5.3 Algoritmik Doğrulayıcı Seçimi

Doğrulama protokolü tutarlı özetleme kullanır [6] (Şek. 4). Doğrulama ücretli bir hizmettir: doğrulayıcılar bir ücret karşılığında çalışır ve rekabetin fiyatlandırmayı, hızı ve güvenilirliği yönlendirdiği bir piyasa oluşturur.

Adım 1. İddia belgesi, önceki yinelemenin özet sonucuyla (veya ilk yinelemede $\emptyset$ ile) birleştirilir ve özetlenir:

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

Algoritma, tüm önceki taleplerin ve yanıtların *tam yolunu* içermelidir—yalnızca önceki yinelemenin bir özetini değil. Her doğrulayıcının tam yanıtı (kabul, ret, teklif edilen fiyat, gerekçe) büyüyen belgeye eklenir ve her adımda kriptografik imzalarla doğrulanabilir.

Adım 2. Özet, tutarlı özet halkası üzerinde eşit olarak dağıtılmış N konuma eşlenir (ör. $N = 4$ için: $+0^\circ, +90^\circ, +180^\circ, +270^\circ$). Her konumdan saat yönünde bir arama, en yakın DID'i doğrulayıcı adayı olarak seçer (Şek. 5). N , o an etkin olan DID'lerin yüzdesine, günün saatine veya ağın geçmiş yanıt verme durumuna bağlı olabilen değişken bir parametredir.

Adım 3. Doğrulayıcı kabul eder (yayımlar, itibarını ortaya koyar) veya reddeder (ret özetiyle Adım 1'e döner). Bir düğüm çevrimiçi durumunu beyan etmesine rağmen yanıt vermediğinde, sonraki talep önceki N doğrulayıcı adayının tüm yanıtlarını içermelidir.

Asalaklığı önleme. Hedef DID'ler, az itibarı olan yeni DID'lerden gelen sorgular için ücretler veya erişim kısıtlamaları belirleyebilir. Bu kademeli mekanizma (ikili değil) yeni katılanları, başkalarının verilerini serbestçe tüketmeden önce gerçek etkinlik yoluyla itibar oluşturmaya zorlar.

Her ret, doğrulayıcının tam yanıtını (gerekçeler ve koşullar dahil) iddia belgesine ekleyerek içeriğini genişletir. Genişletilmiş belgeden, farklı bir halka konumuna eşlenen ve farklı bir doğrulayıcı seçen yeni bir özet deterministik olmayan biçimde hesaplanır. Tam yolun belgelenmesi zorunludur—ihraççı bir sonraki doğrulayıcıyı öngöremez veya etkileyemez. Uyumlu bir beyan edilmiş politikaya rağmen bir doğrulayıcı bir

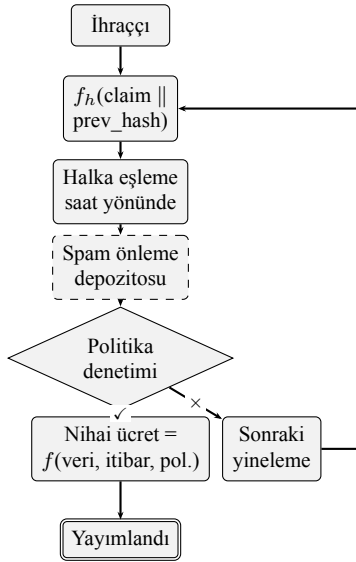


Figure 4: Doğrulayıcı seçim protokolü. Spam önleme depozitosu isteğe bağlıdır ve iade edilebilir. Nihai ücret yalnızca kabul üzerine ödenir.

talebi görmezden gelirse, tanıklar (varsa) bunu kaydedebilir ve ihraççı nihai yayımlama sırasında tanık kanıtı ekleyebilir.

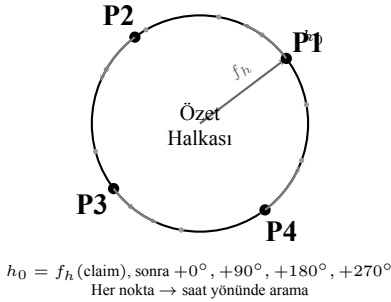


Figure 5: Çok noktalı seçim ($N=4$). h_0 özeti kaymayı belirler; h_0 'dan eşit dağıtılmış 4 nokta.

5.4 Tanık Protokolü

Tanık rolü, kriptografik bir meydan okuma kodu protokolü aracılığıyla doğrulayıcı dürüstlüğü için gizli hesap verebilirlik sağlar:

Adım W1. Talep eden, doğrulama talebini imzalar ve N_w tanığa gönderir—talep edenin sosyal ağından kişiler veya ücret karşılığında çalışan uzman tanık hizmeti sağlayıcıları.

Adım W2. Her tanık w_i , imzalanmış talebin tamamını imzalar, orijinal imzayı σ_i saklar ve bir meydan okuma kodu $c_i = h(\sigma_i)$ hesaplar. Meydan okuma kodu talebe eklenir.

Adım W3. Artık N_w meydan okuma kodu taşıyan talep, doğrulayıcıya gönderilir. Doğrulayıcı kodları

görür ancak tanıkların kim olduğunu veya kodların gerçek imzalara karşılık gelip gelmediğini *belirleyemez*.

Adım W4 (dürüst doğrulayıcı). Doğrulayıcı beyan ettiği politikaya göre yanıt verirse, meydan okuma kodları opak kalır. Tanıklar asla açığa çıkmaz. Ek veri yayımlanmaz.

Adım W5 (politika ihlali). Doğrulayıcı politikasını ihlal ederse (talebi görmezden gelir, tutarsız yanıt verir), talep eden tanıkların orijinal imzaları σ_i 'yi elinde tutar. Bunlar yardımcı veri olarak yayımlanabilir: herkes $c_i = h(\sigma_i)$ 'yi doğrulayabilir ve tanığın hazır bulunduğunu kanıtlayabilir. Talep eden bağımsız olarak yayımlayabilir—doğrulayıcı zaten yanıtında meydan okuma kodlarını imzalamıştır.

Blöf özelliği. Talep eden, meydan okuma kodlarının bazıları veya tümü için rastgele değerler koyabilir. Doğrulayıcı gerçek kodları (yüksek itibarlı otoritelere desteklenen) gürültüden ayırt edemez. Bu *belirsizlik*, uygulama mekanizmasıdır: her talep, saygın bir otoritenin gizlice izliyor olması riskini taşır. Bu baskıyı sürdürmenin maliyeti sıfıra yakındır (rastgele sayılar üretmek), oysa doğrulayıcı için sahtekârlığın potansiyel maliyeti felakettir. Gerçek tanıkların yokluğunda bile dürüst davranış teşvik edilir.

Tanık olarak otorite. Bir iddiayı onaylayan bir Otorite tanık hizmetlerini birleştirebilir: “İddianızı onaylıyorum ve doğrulama sırasında gizli tanık olarak hizmet ediyorum.” Bu doğal bir iş modelidir—Otorite zaten bağlama sahiptir. Ancak iki rol mantıksal olarak bağımsızdır.

5.5 Pahalı Radikallik İlkesi

Üç maliyet kanalı aynı anda birleşerek büyür (Şek. 6):

Kanal 1: Yineleme Maliyeti. Her ret, zaman ve kaynak tüketen yeni bir yinelemeyi zorunlu kılar. Doğrusal büyüme.

Kanal 2: Belge Şişmesi. Her yineleme, tam doğrulayıcı yanıtını iddia belgesine ekler. Büyüme doğrusaldır ancak bir taban ofsetiyle: başlangıç yükü (iddia içeriği, otorite onayı, kriptografik imzalar) zaten önemsiz olmayan bir B_0 boyutuna sahiptir. k yinelemeden sonraki toplam boyut: $S(k) = B_0 + k \cdot \Delta$, burada Δ ortalama yanıt boyutudur.

Kanal 3: Doğrulayıcı Risk Primi. Risk öznelidir. Doğrulayıcı, talep eden DID'in beyan ettiği politikaların doğrulayıcının kendi ticari, sosyal veya siyasî çıkarlarıyla çatışıp çatışmadığını değerlendirir. Prim, doğrulayıcının “ideali”nden algılanan uzaklıkla üstel olarak yükselebilir: $P(d) = \alpha \cdot e^{\beta d}$, burada d doğrulayıcının öznel uzaklık ölçütüdür. Kişisel bir yasak

sınırının ötesinde, doğrulayıcı tamamen reddedebilir.

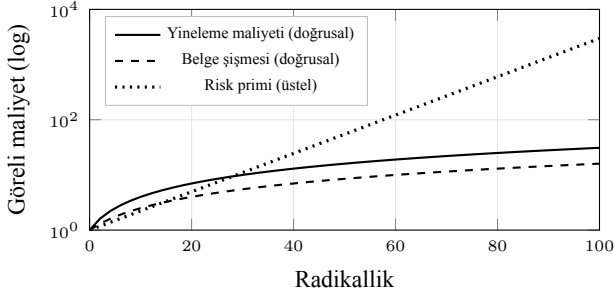


Figure 6: Üç kanal boyunca maliyet artışı. Risk primi yüksek radikallikte baskın gelir.

Kritik olarak, bu sansür değildir. Hiçbir iddia yasaklanmaz. Sistem riski fiyatlandırır (Tablo 1).

Table 1: İddia türleri arasında maliyet karşılaştırması.

Tür	Yin.	Belge	Ücret	Toplam
İnandırıcı	$k_{\min}$	B_0	$P_{\min}$	Düşük
Tartışmalı	k_{med}	$B_0 + k\Delta$	$\alpha e^{\beta d}$	Orta
Radikal	$k_{\max}$	$\gg B_0$	$\gg P_{\min}$	Çok yüksek
Sahtekârca	$\rightarrow \infty$	—	—	Yayımlanamaz

6 İtibar ve Risk Değerlendirmesi

6.1 İtibar Birikim Modeli

İtibar üç özellik sergiler: **yavaş birikim** (tutarlı davranışla kademeli büyüme), **hızlı yıkım** (tek bir sahtekârlık puanı felaket derecesinde düşürebilir) ve **bireysel değerlendirme** (her tüketici taraf kendi toplama işlevini uygulayabilir).

6.2 İtibarlı Otoriteler

Bir İtibarlı Otorite iddiaları inceler ve tatmin olursa onları ortak imzalar—kendi itibarını ortaya koyar (Şek. 7). Asimetri tasarım gereğidir: itibar kazanmak yavaştır (dürüst onay başına kademeli $+\delta$), kaybetmek ise felakettir (sahte onay başına $-\Delta \gg \delta$; örnekleme amacıyla, ör. $+2\%$ 'ye karşı -70%). Optimal strateji her zaman şüpheli iddiaları reddetmektir. δ ve Δ 'nın özgül değerleri sistem parametreleridir.

6.3 Çok Boyutlu İtibar

İtibar bir skaler değil, birden çok boyutta bir vektördür: malî güvenilirlik, kişisel dürüstlük, mesleki yeterlilik, sivil katılım ve diğerleri (Şek. 8). Farklı değerlendirme sağlayıcıları bu vektörü bağlama bağlı olarak farklı

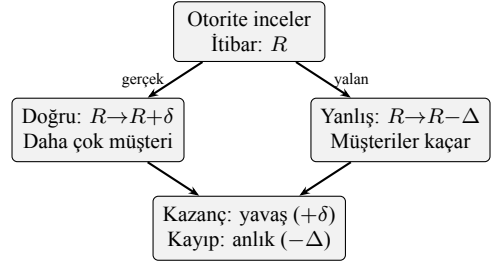


Figure 7: İtibarlı Otorite—asimetrik teşvikler.

biçimde yansıtır—bir kredi veren malî güvenilirliği önceler, bir işveren mesleki yeterliliği, bir komşu sivil davranışı. Tek bir “doğru” itibar puanı yoktur; yalnızca bakış açıları vardır.

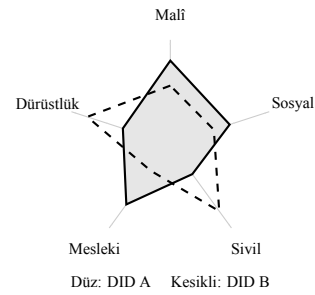


Figure 8: Çok boyutlu itibar vektörleri. Farklı DID'ler boyutlar arasında farklı profiller sergiler.

6.4 Demokratikleştirilmiş Risk Değerlendirmesi

RSN, sistematik risk değerlendirmesini demokratikleştir—şu anda malî kurumlarda yoğunlaşan ancak bankacılığın çok ötesinde uygulanabilir bir yetenek. Tedarikçi güvenilirliğini değerlendiren sınıai holdingler, davranışsal riski fiyatlandıran sigorta şirketleri, birleşme ve devralmalar için durum tespiti, imalatla ekipman ömrü tahmini—karşı taraf riskinin değerlendirilmesi gereken her yerde RSN, merkeziyetsiz, piyasa güdümlü bir alternatif sağlar. Bir yorum hizmetleri piyasası, hem çok boyutlu itibar verilerini eyleme geçirilebilir özetlere çevirir ve karşı taraf değerlendirmesini herhangi bir katılımcı için marjinal maliyetle erişilebilir kılar.

7 Uzlaşa ve Uyuşmazlık Çözümü

7.1 Merkeziyetsiz Adalet Modeli

RSN, adaleti iki yönlü bir pazarlık sorunu olarak yeniden çerçeveler. Kalıcı, doğrulanabilir itibar zararı tehdidi, zarar gören tarafın karşılayamayacağı yasal süreçlerden daha etkili bir caydırıcıdır.

7.2 Kendiliğinden Oluşan Uzlaş

Her katılımcı kişisel bir tatmin eşiği tutar. Ağın toplu uzlaşısı, binlerce iki yönlü pazarlığın istatistiksel ortalaması olarak ortaya çıkar (Şek. 9). Uzlaşının çok üzerinde bir yanıt (barbarca) yayımlaması pahalıdır. Uzlaşya yakın bir yanıt (orantılı) ucuzdur. Uzlaş bir kural değildir—bir fiyat sinyalıdır.

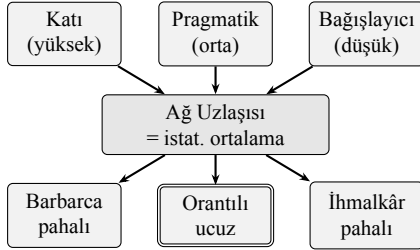


Figure 9: Bireysel tatmin eşiklerinden kendiliğinden oluşan uzlaş.

7.3 Cezanın Ayarlanması

Her DID Sahibi belirli kötü davranış kategorilerine yönelik yanıtlarını kamuya açık olarak beyan eder. Orantısız derecede sert veya hoşgörülü beyanlar olumsuz itibar sinyalleri çeker. Orantılı beyanlar sürtünmesiz kabul edilir—kendini kalibre eden bir ceza sistemi.

Uzlaş beyanları da ikiyüzlülük tespitine tabidir: bir uzlaş pozisyonuna beyanen bağlanırken tutarsız davranmak, kasıtlı aldatmayı gösterdiği için temeldeki sapmadan daha ağır bir itibar suçu oluşturur.

7.4 Devir

Bir DID içindeki tüm etkinlikler—bir istisna dışında—başka bir DID’e devredilebilir. **Özne rolü—davranış iddianın konusu olan DID—devredilemez; iddianın atıfta bulunduğu kimlik sahibine devredilemez biçimde bağlıdır.** Diğer etkin roller—İhraççı, Otorite, Tanık, Doğrulayıcı—ister doğrulama, ister iddia sunma, ister uzlaş katılımı, ister uyumsuzluk çözümü için olsun, belirlenmiş bir vekil DID’e aktarılabilir. Devir her an geri alınabilir. Bu, Sahibin nihai denetimi ve sorumluluğu elinde tutmasını sağlarken uzmanlaşmaya (ör. profesyonel doğrulama hizmetleri) olanak tanır. Devir tüm sistem boyunca geçerlidir ve ölçeklenebilirlik için elzemdir.

7.5 Bireysel Ahlaktan Kendiliğinden Oluşan Toplumsal Sözleşmeye

Her DID’in beyan ettiği politika, bireysel ahlakın bir formülleşmesini temsil eder: Sahibin neyi kabul

edilebilir gördüğü, belirli davranışlara nasıl yanıt verdiği, karşı taraflardan ne talep ettiği. Bu politikalar bir sistem tasarımcısı tarafından dayatılmaz—her katılımcı tarafından seçilir ve makinece okunabilir biçimde ifade edilir.

Bu formülleştirme üç aşamalı bir kendiliğinden oluşumu mümkün kılar. Birincisi, bireysel ahlak **politika** olarak kodlanır—DID’in uymayı taahhüt ettiği beyan edilmiş kurallar, eşikler ve yanıt işlevleri dizisi. İkincisi, ağdaki tüm politikaların toplamı **kendiliğinden oluşan etik** üretir—tek bir katılımcının tasarlamadığı ancak binlerce bireysel ahlakî pozisyonun etkileşiminden doğan, istatistiksel olarak gözlemlenebilir normlar [9]. Üçüncüsü, iki yönlü fiyat sinyalleri aracılığıyla uygulanan paylaşılan davranış normları olarak ifade edilen bu kendiliğinden oluşan etik, **ölçülebilir bir toplumsal sözleşme** oluşturur—kimsenin imzalamadığı teorik bir kurgu değil [10], gerçek davranışla desteklenen, ampirik olarak gözlemlenebilir bir kurallar dizisi.

Bu süreç ahlakî temeller kuramının bulgularını yansıtır [11]: insan ahlakı sezgisel, çoğulcu ve kültürel olarak değişkendir. RSN bir girdi olarak ahlakî uzlaş gerektirmez; bir çıktı olarak davranışsal uzlaş üretir. Ortaya çıkan toplumsal sözleşme statik değildir—katılımcılar katıldıkça, ayrıldıkça ve ağ geri bildirimine yanıt olarak politikalarını ayarladıkça evrilir. Klasik toplumsal sözleşme kuramının aksine, bu sözleşme geri alınabilir, gözlemlenebilir ve bir hükümdar olmaksızın uygulanabilir.

8 Ekonomik Model

Önceki bölümler bir aracı—RSN’nin doğrulama mekanizmalarını, maliyet yapısını ve kendiliğinden oluşan uzlaşısını—tanımladı. Bu bölüm, bu aracın malî ve yönetsel geçişe uygulanması için bir metodoloji tanımlar. Araç genel amaçlıdır; aşağıdaki metodoloji olası bir uygulamadır.

8.1 Teşvik Yapısı

Sermaye olarak itibar, dürüst davranış için doğru teşvikler oluşturur. Normal işleyişte katılımcılar itibarı günlük işlemler ve yerine getirilen taahhütler yoluyla doğal olarak oluşturur. Birincil harcama *olumsuz* iddialardır—başkalarının verdiği zararı kaydetmek. Bu asimetri, yararlı, güvenilir davranış teşvik eder: dürüst olmanın ek maliyeti yoktur, zararlı olmak ise başkalarının korumak için ödeme yapacağı belgelenmiş bir iz oluşturur. İkiyüzlülük—kurallara uymadan onları beyan etmek—kasıtlı aldatmayı gös-

terdiği için en maliyetli başarısızlık biçimidir.

8.2 Paralel Malî Sistem

Üç bileşen rekabetçi baskı sağlar: (1) **Basit Vergi**—istisnasız, tek oranlı, başlangıçta mevcut fiilî oranın marjinal olarak altında bir orantılı vergi; (2) **Elektronik Harcama Kaydı (ESR)**—Çek EET modelini tersine çevirerek vatandaşların devlet harcamalarını denetlemesini sağlar; (3) **Vatandaş Yönlendirmeli Vergi Tahsisi**—ilk yılda birkaç yüzde ile başlar ve on yıl sonra, benimseme hızına bağlı olarak düşük çift haneli rakamlardan vatandaş yönlendirmeli bir sisteme tam geçişe kadar herhangi bir yere ulaşır. Fiilî tempo, devlet hizmetlerine serbest piyasa alternatiflerinin ortaya çıkma hızına ve devletin geçişle iş birliği yapma isteğine bağlıdır; zamanın işlevinin doğrusal olması gerekmez ve benimsemenin nihayetinde nereye varabileceğine bir üst sınır koymak için hiçbir neden yoktur.

9 Geçiş Yolu

Geçiş üç aşamadan geçer (Şek. 10): **Aşama 1: Örtü** (bilgi katmanı olarak RSN, devlet tek sağlayıcı), **Aşama 2: Rekabet** (RSN işlevsel alternatifler sağlar, çift sistem kullanımı) ve **Aşama 3: Geçiş** (RSN devlet eşdeğerlerinden daha iyi performans gösterir, gönüllü göç). Geçiş her aşamada geri döndürülebilir.

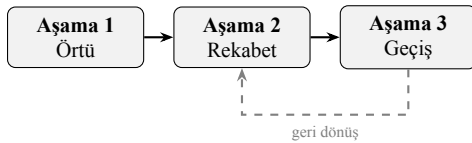


Figure 10: Üç aşamalı geçiş—her aşamada geri döndürülebilir.

Birincil baskı mekanizması malîdir: koşullu vergi mükellefleri “ekonomik olarak önemli bir azınlık X ”e ulaştığında—ona karşı baskı önemsiz olmayan ekonomik zarara yol açacak ve sivil itaatsizliğin inandırıcı bir tehdit haline geleceği kadar büyük bir grup—devlet müzakereye girer. Örneklem amacıyla $X \approx 15\%$ (GSYİH’nin) kullanıyoruz, ancak fiilî eşik belirli ekonomiyeye bağlıdır.

10 Güvenlik Analizi

Beş düşman kategorisini ele alıyoruz: bireysel kötü niyetli aktörler, örgütlü gruplar, kurumsal düşmanlar,

devlet düzeyindeki düşmanlar ve protokol düzeyindeki düşmanlar.

Sybil direnci [12]. İtibar oluşturmak, sürekli, doğrulanabilir etkileşim gerektirir. Başarılı bir Sybil saldırısının maliyeti, sahte kimliklerle doğrusal ve hedef itibar düzeyiyle karesel olarak ölçeklenir. Paralel olarak birden çok DID işletmek mümkündür ancak tasarım gereği pahalıdır—her kimlik, gerçek etkinlik yoluyla bağımsız olarak itibar biriktirmelidir. Özgür toplumlarda bu maliyet gelişigüzel istismarı caydırır; diktatörlüklerde ise paralel DID’ler, bölmelenmiş direnişi, yeraltı koordinasyonunu ve daha güvenli karaborsa gezinmesini mümkün kılan bir hayatta kalma aracı haline gelir.

Gizli anlaşma savunması. Kapalı gruplar arasındaki karşılıklı onay örüntüleri, sosyal grafik analizi yoluyla tespit edilebilir. İtibar toplama işlevleri, sıkı biçimde kümelenmiş kaynaklardan gelen iddiaları iskonto eder.

Devlet düzeyinde düşman. Soğan yönlendirmesi, merkezî altyapının yokluğu ve Doğrulamalı rolünün katılımcı tabanına dağıtılması, bastırmanın herhangi bir yararla orantısız önlemler gerektirmesini sağlar.

Mahremiyete karşı hesap verebilirlik. Takma adlılık—anonimlik ile kimlik ifşası arasında bir orta yol—DID’lerin Sahibin gerçek dünyadaki kimliğini açığa çıkarmadan anlamlı itibar biriktirmesine olanak tanır.

11 Mahremiyet Değerlendirmeleri

RSN’nin mahremiyet modeli takma adlılık üzerine kuruludur. Sahip kimlik ifşasını denetler: asgari (saf takma ad), seçici (belirli kimlik bilgileri bağlı) veya tam (yasal kimlik ilişkilendirilmiş). Yayımlanan iddialar kalıcıdır—sistem bağlamsal düzeltmeyi destekler ancak silmeyi desteklemez. Bir Sahip, biriktirilen itibarı feda ederek tehlikeye girmiş bir DID’i terk edip yeniden başlayabilir.

12 İlgili Çalışmalar

W3C DID Core spesifikasyonu [2] ve Ceramic Network [8] kimlik temelini sağlar. EigenTrust [13] merkezî otorite olmaksızın dağıtık itibar toplamasını gösterdi. SBT’ler [3] devredilemez sosyal belirlenimleri tanıttı. RSN, bir kalite filtresi olarak ekonomik maliyete vurgusu ve radikalliği fiyatlandırma mekanizmasıyla farklılaşır.

DAO’lar [4] ve karesel oylama [5] merkeziyetsiz yönetimin uygulanabilirliğini gösterdi. RSN uzlaşmayı

oynamadan ziyade iki yönlü fiyat pazarlıklarından türetilir.

Öneri, özel hizmet sağlama için anarko-kapitalist kuramdan [14, 15] yararlanır ancak iki kritik açıdan ayrılır: rasyonellik varsaymak yerine kin ve intikam dürtüleri için tasarım yapar ve devrim yerine kademeli geçiş önerir. Kendiliğinden oluşan toplumsal sözleşmeler kavramının, Hayek'in kendiliğinden düzen kuramında [16] öncülleri vardır.

Anarko-agorizm. RSN, agorist karşı-ekonomi ile [17]—özellikle paralel kurumlar inşa etmeye ve gönüllü değişime yaptığı vurguyla—önemli bir ortak zemin paylaşır. Ancak agorizm, rasyonel öz-çıkartı yeterli bir koordinasyon mekanizması olarak varsayma eğilimindedir ve genellikle mevcut devlet yapılarından somut bir geçiş yolundan yoksundur. RSN, rasyonel olmayan davranışsal eğilimleri açıkça bünyesine katar ve kademeli geçiş için malî bir baskı mekanizması sağlar.

Liyakat sistemi. RSN, liyakatin [18] bir slogan yerine sistemik bir özellik olarak nasıl ortaya çıkabileceğine dair ilk işlevsel tanımı temsil edebilir. Geleneksel liyakat sistemleri başarısız olur çünkü “liyakati” tanımlayacak ve uygulayacak merkezî bir otorite gerektirir. RSN’de liyakat iki yönlü değerlendirmelerden ortaya çıkar: değer sunanlar itibar biriktirir; kimin liyakatli olduğuna hiçbir komite karar vermez.

Ayrıcalık olarak mülkiyet. RSN, mülkiyet haklarına doğal ve mutlak olarak yaklaşan anarko-kapitalist ve Avusturya okulu yaklaşımlarından temelde ayrılır. RSN çerçevesinde mülkiyet bir *ayrıcalıktır*—bir katılımcı paylaşılan normları temelden ihlal ettiğinde (ihamet, varoluşsal krizde topluluğu savunmayı reddetme, sistematik sömürü) uç durumlarda topluluk tarafından geri çekilebilen bir toplumsal tanınma. Bu, devlet kamulaştırması değil, iki yönlü ilişkiler ağı tarafından toplumsal tanınmanın geri çekilmesidir.

13 Tartışma ve Sınırlamalar

Soğuk başlangıç. RSN’nin değeri ağ etkilerine bağlıdır; erken benimseyenler, katılım bir eşiğe ulaşana dek sınırlı değerle karşı karşıya kalır. Ancak erken aşamalardan itibaren bile DID ağı yararlı bir tamamlayıcı bilgi kaynağı olarak hizmet eder. Erken itibar değerlendirmesi ve otorite değerlendirmesinin artan gelişmişlikle kademeli olarak gelişmesi beklenir.

Asalaklığı önleme ve erişim denetimi. Hedef DID’ler, düşük itibarlı DID’lerden gelen sorgulara

kademeli ücretler ve erişim kısıtlamaları getirebilir. Bu ikili değil sürekli bir ölçektir: sorgulayan bir DID’in itibarı ne kadar azsa, o kadar az bilgi alır, o kadar uzun bekler ve o kadar çok öder. Bu mekanizma, edilgen tüketim yerine gerçek katılımı teşvik eder.

Erişim eşitsizliği. İddia yayımlama maliyeti, ekonomik olarak dezavantajlı katılımcıların meşru şikâyetlerini süzebilir. Hafifletme: her katılımcı aynı zamanda potansiyel bir doğrulayıcı olarak hizmet eder (veya bu rolü devreder) ve doğrulama ücretleri kazanır. Yeterli bir zaman ufkunda, radikal olmayan bir katılımcı malî tarafsızlığa yaklaşmalıdır—doğrulama geliri yayımlama maliyetlerini yaklaşık olarak dengeler. Bu bir garanti değil, istatistiksel bir beklentidir.

İtibar eşitsizliği. Erken benimseyenler, geç kalanlar için engeller oluşturabilecek avantajlar biriktirir. Ancak itibar değerlendirmesi, toplama algoritmaları aracılığıyla ilk hamle avantajını hafifletmeyi seçebilecek üçüncü taraf sağlayıcılar tarafından yapılır. İyi bir itibarla ilk olmak meşru bir karşılaştırmalı ekonomik avantajdır—ve bu tasarım gereğidir.

Açık sorular. Optimal maliyet işlevleri, toplama standartları, protokol yönetimi ve yapay zekâ tarafından üretilen sentetik itibar verileriyle etkileşim gelecekteki çalışma alanları olarak kalır.

Bu makale, RSN’nin her koşulda optimal sonuçlar üreteceğini iddia etmez. RSN’nin *uygulanabilir* bir alternatif temsil ettiğini iddia eder—teknik olarak uygulanabilir, ekonomik olarak kendi kendini sürdürebilir ve insan davranış eğilimleriyle gerçekte oldukları haliyle sosyal olarak uyumlu.

14 Sonuç

Bu makale, takma adlı, doğrulanabilir itibar değişimini mümkün kılan merkeziyetsiz bir protokol olan İtibar Sosyal Ağı’nı sundu. Pahalı Radikalite İlkesi, sahtekârca iddiaların sansür olmaksızın fiyat yoluyla dışlanması sağlar. Önerilen geçiş yolu, mevcut kurumlardan kademeli, geri döndürülebilir bir geçişi mümkün kılar. Tasarım, ideolojik dönüşüm gerektirmek yerine insan doğasını olduğu haliyle—küçüklük, kin ve intikam alma tatmini arzusu dahil—bünyesine katar. Sonuç bir ütopya değil, adaletin erişilebilir olduğu, itibarın hak edildiği ve kötü davranışın maliyetinin ona neden olan tarafça üstlenildiği bir sistemdir.

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. Ohlhaver, 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.