Jaringan Reputasi Terdesentralisasi: Kerangka Kerja untuk Organisasi Sosial Alami

Pavel Kudrna
Prague, Czechia
Draft v1 — March 2026

Abstract

Rasa keadilan—keyakinan bahwa kesalahan diperbaiki dan jasa dihargai—adalah kekuatan kohesif terkuat dalam masyarakat. Ketika institusi tata kelola yang tersentralisasi tidak dapat memberikan rasa ini karena biaya menegakkan suatu hak melebihi nilai hak itu sendiri, kohesi sosial pun terkikis. Struktur institusional saat ini gagal menyelesaikan sekelompok besar sengketa dengan cara yang secara sistematis sama seperti perencanaan terpusat gagal mengalokasikan sumber daya: melalui asimetri informasi, hilangnya lingkaran umpan balik, dan terputusnya pengambil keputusan dari konsekuensi keputusan mereka. Makalah ini menyajikan Reputation Social Network (RSN): sebuah lapisan komunikasi yang terdesentralisasi, tidak dapat dikorupsi, dan tahan sensor yang dibangun di atas Decentralized Identifiers (DIDs) yang memungkinkan peserta pseudonim untuk memublikasikan, memverifikasi, dan mengonsumsi informasi reputasi tentang perilaku di dunia nyata. Mekanisme inti bertumpu pada tiga prinsip desain: (1) struktur biaya asimetris di mana membaca data reputasi itu murah tetapi menulis memerlukan upaya yang dapat diverifikasi; (2) protokol pemilihan verifikator nondeterministik berbasis consistent hashing yang menetapkan harga bagi klaim radikal melalui biaya iterasi yang meningkat; dan (3) model otoritas reputasi berbasis pasar di mana verifikator swasta mempertaruhkan reputasi yang telah mereka kumpulkan atas keakuratan klaim yang mereka dukung. Arsitektur yang dihasilkan menghasilkan meritokrasi yang muncul secara emergen tanpa koordinasi terpusat dan memungkinkan jalur migrasi yang bertahap dan dapat dibalik dari sistem yang saat ini dikelola negara.

1 Pendahuluan

1.1 Masalah Kepercayaan Tersentralisasi

Tata kelola modern bertumpu pada asumsi fundamental: bahwa institusi tersentralisasi dapat memediasi kepercayaan antara orang asing dalam skala besar. Pengadilan mengadili sengketa. Registri menyertifikasi kepemilikan. Badan regulasi menegakkan standar. Institusi-institusi ini dirancang pada era ketika informasi langka, komunikasi lambat, dan pendelegasian wewenang kepada badan pusat adalah satu-satunya mekanisme koordinasi yang layak. Namun, tata kelola tersentralisasi gagal karena alasan struktural yang sama seperti perencanaan terpusat: asimetri informasi, hilangnya lingkaran umpan balik, dan terputusnya pengambil keputusan dari konsekuensi keputusan mereka.

Asumsi ini gagal, misalnya, ketika biaya mediasi institusional melebihi nilai sengketa. Bayangkan seorang penyewa yang menemukan bahwa apartemen sewaannya tidak memiliki sertifikat keselamatan listrik yang diwajibkan hukum—suatu kondisi yang menimbulkan bahaya langsung bagi nyawa. Hak hukum penyewa untuk membatalkan kontrak sudah jelas tanpa keraguan. Namun biaya menegakkan hak tersebut melalui sistem pengadilan melebihi nilai moneter dari deposit dan ganti rugi yang terutang, bahkan termasuk potensi kompensasi menurut undang-undang [1]. Respons yang rasional adalah menanggung kerugian dan pergi.

Ini bukanlah kasus tepi yang patologis. Ini adalah pengalaman default untuk sekelompok besar sengketa di mana kerugiannya nyata tetapi taruhan moneternya berada di bawah ambang batas di mana penegakan institusional menjadi rasional secara ekonomi. Hasilnya adalah sebuah sistem yang secara struktural menguntungkan pelaku jahat: mereka yang merugikan orang lain dalam volume di bawah ambang batas ini dapat bertindak tanpa hukuman, karena biaya mencari keadilan jatuh pada pihak yang dirugikan.

Contoh di atas diambil dari lingkungan hukum penulis—sistem hukum perdata Ceko. Dalam tradisi hukum lain—common law berbasis preseden, hukum adat, sistem campuran—keadilan gagal dengan cara yang berbeda dan pada tingkat yang berbeda, tergantung pada kekhususan budaya dan prosedural yurisdiksi tersebut. Pembaca kemungkinan akan mengenali contoh serupa dari konteks mereka sendiri. Yang bersifat universal secara struktural adalah polanya: sengketa yang nilainya jatuh di bawah ambang batas penegakan yang rasional secara ekonomi berakhir dengan kerugian yang ditanggung oleh pihak yang dirugikan. RSN tidak menjanjikan keadilan yang sempurna—ia hanya mengurangi keunggulan struktural yang dinikmati pelaku jahat ketika penegakan institusional tidak ekonomis.

1.2 Mengapa Solusi yang Ada Belum Memadai

Kerangka Decentralized Identity (DID) [2] menyediakan mekanisme kriptografis untuk manajemen identitas berdaulat-sendiri tetapi berfokus terutama pada verifikasi identitas tanpa membahas pertanyaan yang lebih luas tentang reputasi perilaku.

Soulbound Tokens (SBTs) [3] menangkap wawasan bahwa reputasi tidak dapat dipindahtangankan tetapi bergantung pada infrastruktur blockchain dengan keterbatasan skalabilitas dan tidak membahas insentif ekonomi yang mengatur pemasukan informasi. Konsep terkait seperti merit token (mis., Liberland) memiliki filosofi serupa tetapi tetap terikat pada kerangka yurisdiksi tertentu.

Decentralized Autonomous Organizations (DAOs) [4] menerapkan tata kelola melalui smart contract tetapi mereplikasi dinamika plutokratik di mana pengaruh sebanding dengan modal. Quadratic voting [5] sebagian mengurangi hal ini tetapi membatasi adopsi praktis. DAO juga menghadapi *masalah oracle* yang fundamental: smart contract tidak dapat memverifikasi keadaan dunia nyata secara andal tanpa sumber eksternal yang tepercaya, dan masalah ini tidak memiliki solusi umum dalam arsitektur blockchain.

Tidak ada sistem yang ada yang menggabungkan desentralisasi, ketahanan terhadap sensor, pseudonimitas, biaya masuk yang dapat diverifikasi, dan konsensus yang emergen.

1.3 Kontribusi

Makalah ini memberikan kontribusi sebagai berikut:

1. Definisi **Reputation Social Network (RSN)**, sebuah protokol terdesentralisasi yang memperluas kerangka DID untuk mendukung pertukaran reputasi bilateral.
2. Sebuah **protokol pemilihan verifikator nondeterministik** berbasis consistent hashing [6].
3. **Prinsip Radikalisme yang Mahal**, yang menetapkan harga klaim menurut jaraknya dari konsensus jaringan melalui tiga saluran biaya yang bergabung.
4. Sebuah **model Otoritas Bereputasi** dengan insentif asimetris di mana dukungan palsu berbiaya jauh lebih besar secara katastrofik daripada biaya yang sah.
5. Sebuah **jalur migrasi bertahap** melalui infrastruktur fiskal paralel.

2 Prinsip Desain

Arsitektur RSN dibatasi oleh lima prinsip desain yang tidak dapat ditawar.

Kontinuitas dan Evolusi. Sistem ini berdampingan dengan institusi yang ada selama periode transisi dengan durasi yang tidak ditentukan. Transisi tersebut harus dapat dibalik pada setiap tahap.

Kesukarelaan dan Tanggung Jawab. Partisipasi bersifat sukarela, tetapi kesukarelaan dipadukan dengan tanggung jawab: seorang peserta yang mengambil kendali atas suatu fungsi institusional secara bersamaan mengambil kewajiban yang menyertainya.

Keberagaman dan Netralitas Budaya. Konsensus muncul dari interaksi bilateral, bukan dari aturan yang ditetapkan sebelumnya yang dipaksakan oleh perancang sistem.

Ketahanan dan Ketahanan terhadap Sensor. Biaya menyensor jaringan harus melebihi biaya menoleransinya. Hanya totalitarianisme penuh—dengan biaya politik dan ekonomi yang menghancurkan—yang dapat menekan sistem ini.

Konsensus dan Penegakan. Sistem ini menyertakan kecenderungan manusia terhadap kepicikan, kedengkian, dan kepuasan pembalasan sebagai fitur penopang beban. Pelanggaran tidak dilarang; ia diberi harga.

3 Gambaran Umum Sistem

3.1 Reputation Social Network

RSN adalah lapisan komunikasi peer-to-peer yang terdesentralisasi di mana peserta bertukar informasi

yang dapat diverifikasi tentang perilaku di dunia nyata. Sifat-sifat yang mendefinisikannya adalah: infrastruktur yang terdesentralisasi dan tidak dapat disensor; partisipasi pseudonim melalui DID; struktur biaya asimetris (membaca murah, menulis mahal); keterverifikasian kriptografis; dan **dukungan standar**—format yang dapat dibaca mesin untuk informasi yang disebarkan melalui jaringan, untuk layanan yang ditawarkan oleh otoritas (penyusunan klaim, dukungan, layanan saksi), dan untuk format kebijakan termasuk aturan untuk mengevaluasi reputasi pihak lawan serta menilai risiko ketidaksesuaian kebijakan (antara perilaku yang dinyatakan dan yang sebenarnya).

3.2 Komponen Arsitektural

RSN terdiri dari empat komponen utama (Gbr. 1):

1. **Lapisan DID.** Identitas peserta dengan aturan yang dinyatakan, metadata reputasi, dan perutean jaringan.
2. **Protokol Klaim.** Format terstruktur untuk memublikasikan pernyataan tentang peristiwa dunia nyata.
3. **Jaringan Verifikasi.** Protokol terdesentralisasi untuk menugaskan verifikator menggunakan consistent hashing.
4. **Lapisan Agregasi Reputasi.** Layanan yang menghasilkan ringkasan reputasi yang dapat dibaca manusia.

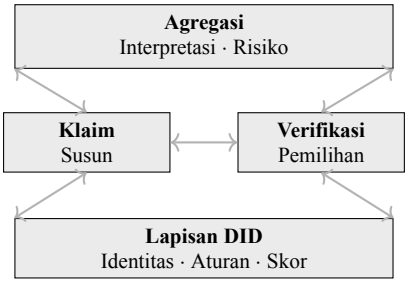

Figure 1: Arsitektur empat lapisan RSN.

3.3 Peran Peserta

Sebuah transaksi verifikasi melibatkan hingga enam peran DID yang berbeda (Gbr. 2): **Penerbit** (DID_I, membuat dan mengajukan klaim), **Subjek** (DID_S, DID yang menjadi objek klaim—dapat bertepatan dengan Penerbit), **Otoritas** (DID_A, mendukung klaim dengan imbalan; juga dapat menawarkan layanan saksi—*opsional*), **Saksi** ($DID_{W_{1..n}}$, pemantau kejujuran verifikator secara inkognito melalui kode tantangan—*opsional*), **Verifikator** (DID_V, dipilih secara algoritmik untuk memublikasikan klaim), dan **RSN** (jaringan tempat klaim yang terverifikasi dipublikasikan). Peran apa pun dapat didelegasikan ke DID lain (Bagian 7.4). Sebuah Otoritas umumnya menggabungkan dukungan dengan layanan saksi, tetapi kedua fungsi tersebut secara logis independen.

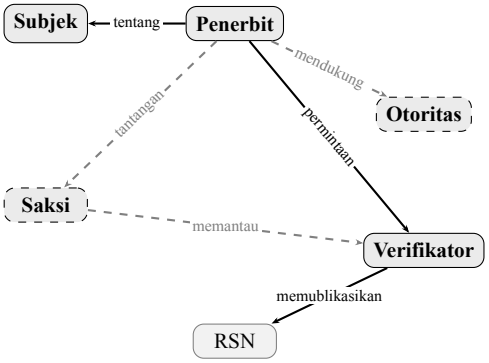

Figure 2: Peran DID dalam sebuah transaksi verifikasi. Garis putus-putus = opsional (Otoritas, Saksi).

3.4 Ketidakterkorupsian: Empat Kekuatan

Ketidakterkorupsian RSN tidak berasal dari satu mekanisme tunggal melainkan dari empat kekuatan yang bersamaan. Tidak ada satu pun yang memadai dengan sendirinya; hanya kombinasinyalah yang membuat upaya korupsi menjadi tidak rasional secara ekonomi.

Target yang tidak dapat diprediksi. Verifikator untuk setiap klaim dipilih secara nondeterministik melalui consistent hashing (Bagian 5.3). Penyerang tidak dapat menargetkan verifikator tertentu untuk suap sebelumnya, karena identitas verifikator merupakan fungsi dari isi klaim dan iterasi sebelumnya, bukan pilihan penerbit.

Pengungkit reputasi—naik lambat, turun cepat. Reputasi hanya dapat diperoleh secara bertahap, melalui perilaku konsisten yang berkelanjutan. Namun, ia dapat hilang secara katastrofik dalam satu dukungan yang curang (Bagian 6.2). Asimetri ini berarti bertahun-tahun reputasi yang terakumulasi dapat dihancurkan oleh satu dukungan yang tidak jujur; strategi optimalnya tetaplah menolak klaim yang mencurigakan.

Janji publik. Setiap Pemegang DID secara publik menyatakan kebijakannya—seperangkat aturan yang dapat dibaca mesin yang mereka janjikan untuk diikuti. Perbedaan antara pernyataan dan perilaku sebenarnya dapat dideteksi dan diberi harga sebagai pelanggaran reputasi yang lebih berat daripada pelanggaran yang mendasarinya (Bagian 7.3). Karena itu, kemunafikan lebih mahal daripada ketidakjujuran langsung.

Asimetri biaya serangan pada mesh. Biaya menyensor atau mengganggu stabilitas jaringan tumbuh secara nonlinear seiring ukuran dan kepadatan jaringan, sementara biaya menoleransinya tetap konstan. Agar sensor menguntungkan, aktor tersentralisasi harus menerapkannya di seluruh jaringan—memerlukan tindakan yang tidak sebanding dengan manfaat apa pun yang dapat dibayangkan (Bagian 10).

4 Model Identitas Terdesentralisasi

4.1 DID dengan Sifat Khusus

RSN memperluas spesifikasi W3C DID Core [2] dengan: **Aturan yang Dinyatakan** (komitmen perilaku yang dapat dibaca mesin), **Metadata Reputasi** (skor perilaku teragregasi), dan **Perutean Jaringan** (gerbang onion yang dapat berubah, terpisah dari posisi ring yang stabil).

4.2 Siklus Hidup Klaim

Sebuah Klaim melalui enam tahap (Gbr. 3): penyusunan, dukungan otoritas opsional, pemilihan verifikator via consistent hashing, keputusan verifikasi (terima atau tolak dengan iterasi), publikasi, dan pembaruan reputasi untuk semua pihak.

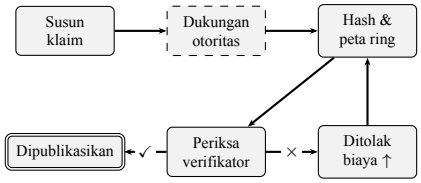

Figure 3: Siklus hidup klaim dengan lingkaran iterasi.

4.3 Hubungan dengan W3C DID Core

Model identitas RSN adalah superset yang tepat dari spesifikasi W3C DID Core [2]. Semua DID RSN adalah DID W3C yang valid. Ekstensi khusus RSN dikodekan sebagai properti dokumen DID yang didefinisikan dalam spesifikasi metode DID khusus, kompatibel dengan infrastruktur yang ada seperti ION [7] dan Ceramic [8].

5 Verifikasi dan Propagasi Informasi

5.1 Biaya Pemasukan Informasi

Prinsip ekonomi inti RSN adalah asimetri antara membaca dan menulis. Membaca data reputasi mendekati biaya marjinal nol bagi peserta yang merupakan bagian dari jaringan DID dan memiliki akses yang sepadan dengan reputasi mereka—pendatang baru harus secara bertahap memperoleh akses yang lebih luas (lihat anti-leeching). Menulis—dipahami sebagai materialisasi reputasi yang tahan lama ke dalam jaringan, bukan sebagai tindakan teknis sekali pakai—memerlukan investasi kumulatif yang dapat diverifikasi di tiga dimensi: **waktu** (bertahun-tahun kehidupan yang dihabiskan untuk perilaku konsisten, komitmen yang dipenuhi, dan hubungan yang dipupuk), **energi** (upaya yang diinvestasikan dalam kejujuran, kepedulian terhadap kemitraan, dan keterpercayaan jangka panjang), dan **uang** (investasi pada nama diri sendiri—pengembangan profesional, kualitas pekerjaan seseorang, restitusi atas kerugian yang ditimbulkan). Reputasi tidak dapat dibeli secara instan—ia adalah hasil dari akumulasi seumur hidup yang hanya dibuat terlihat dan dapat dipindahkan lintas konteks oleh sistem. Biaya teknis sekali pakai dari protokol (tanda tangan kriptografis, biaya verifikator) dapat diabaikan dibandingkan dengan investasi yang mendasarinya ini.

5.2 Grafik Sosial dan Kedalaman Kontak

RSN pada dasarnya adalah jaringan sosial: setiap DID menambahkan kontak (DID lain) yang mengizinkan koneksi tersebut. Kontak-kontak ini memiliki kontak mereka sendiri, dan seterusnya. Pencarian verifikator algoritmik beroperasi dalam kedalaman kontak tertaut yang dapat dikonfigurasi h (mis., $h = 3$: kontak langsung seseorang, kontak mereka, dan kontak dari kontak). Arsitektur ini tidak memerlukan satu blockchain global tunggal—ia secara alami mendukung munculnya komunitas/klaster dengan tumpang tindih ke komunitas lain. Setiap peserta DID harus memiliki **kebijakan** yang dipublikasikan—seperangkat aturan yang dapat dibaca mesin yang mengatur bagaimana permintaan masuk dievaluasi. Pelanggaran kebijakan dicatat dalam jaringan sebagai artefak negatif.

5.3 Pemilihan Verifikator Algoritmik

Protokol verifikasi menggunakan consistent hashing [6] (Gbr. 4). Verifikasi adalah layanan berbayar: verifikator beroperasi dengan imbalan, menciptakan pasar di mana persaingan mendorong penetapan harga, kecepatan, dan keandalan.

Langkah 1. Dokumen klaim digabungkan dengan hasil hash iterasi sebelumnya (atau $\varnothing$ pada iterasi pertama) dan di-hash:

$$\text{pos} = f_h(\text{claim} \| \text{prev\_hash}) \tag{1}$$

Algoritma harus menyertakan *jalur lengkap* dari semua permintaan dan respons sebelumnya—bukan sekadar hash dari iterasi sebelumnya. Respons penuh setiap verifikator (penerimaan, penolakan, harga yang dikutip, alasan) ditambahkan ke dokumen yang terus bertambah, dapat diverifikasi melalui tanda tangan kriptografis pada setiap langkah.

Langkah 2. Hash dipetakan ke N posisi pada consistent hash ring, terdistribusi secara merata (mis., untuk $N = 4$: $+0°, +90°, +180°, +270°$). Dari setiap posisi, pencarian searah jarum jam memilih DID terdekat sebagai kandidat verifikator (Gbr. 5). N adalah parameter variabel yang dapat bergantung pada persentase DID yang sedang aktif, waktu dalam sehari, atau responsivitas jaringan historis.

Langkah 3. Verifikator menerima (memublikasikan, mempertaruhkan reputasi) atau menolak (kembali ke Langkah 1 dengan hash penolakan). Ketika sebuah node tidak merespons meskipun menyatakan status online, permintaan berikutnya harus menyertakan semua respons dari seluruh N kandidat verifikator sebelumnya.

Anti-leeching. DID target dapat menetapkan biaya atau pembatasan akses untuk kueri dari DID baru dengan reputasi kecil. Mekanisme berjenjang ini (bukan biner) memaksa pendatang baru untuk membangun reputasi melalui aktivitas yang tulus sebelum secara bebas mengonsumsi data orang lain.

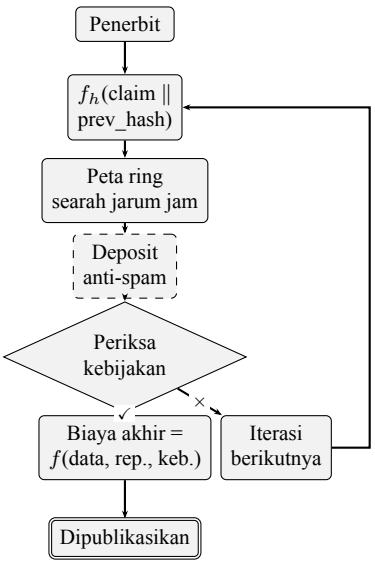

Figure 4: Protokol pemilihan verifikator. Deposit anti-spam bersifat opsional dan dapat dikembalikan. Biaya akhir dibayar hanya pada saat penerimaan.

Setiap penolakan menambahkan respons penuh verifikator (termasuk alasan dan kondisi) ke dokumen klaim, memperluas isinya. Dari dokumen yang diperluas tersebut, sebuah hash baru dihitung secara non-deterministik, dipetakan ke posisi ring yang berbeda dan memilih verifikator yang berbeda. Dokumentasi jalur lengkap bersifat wajib—penerbit tidak dapat memprediksi atau memengaruhi verifikator berikutnya. Jika seorang verifikator mengabaikan permintaan meskipun kebijakan yang dinyatakan kompatibel, para saksi (jika hadir) mencatat hal ini, dan penerbit dapat melampirkan bukti saksi saat publikasi akhir.

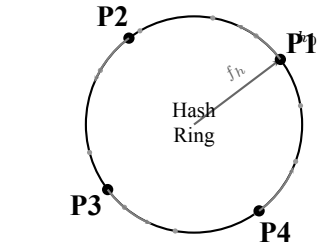

Figure 5: Pemilihan multi-titik (N=4). Hash h_0 menetapkan offset; 4 titik terdistribusi merata dari h_0.

5.4 Protokol Saksi

Peran **Saksi** menyediakan akuntabilitas inkognito untuk kejujuran verifikator melalui protokol kode-tantangan kriptografis:

Langkah W1. Peminta menandatangani permintaan verifikasi dan mengirimkannya kepada N_w saksi—kontak dari jaringan sosial peminta, atau penyedia layanan saksi khusus yang beroperasi dengan imbalan.

Langkah W2. Setiap saksi w_i menandatangani seluruh permintaan yang telah ditandatangani, menyimpan tanda tangan asli σ_i, dan menghitung kode tantangan $c_i = h(\sigma_i)$. Kode tantangan tersebut ditambahkan ke permintaan.

Langkah W3. Permintaan tersebut, yang kini membawa N_w kode tantangan, dikirim ke verifikator. Verifikator mengamati kode-kode tersebut tetapi *tidak dapat menentukan* siapa para saksinya atau apakah kode-kode tersebut sesuai dengan tanda tangan yang nyata.

Langkah W4 (verifikator jujur). Jika verifikator merespons sesuai dengan kebijakan yang dinyatakannya, kode tantangan tetap tidak transparan. Saksi tidak pernah terungkap. Tidak ada data tambahan yang dipublikasikan.

Langkah W5 (pelanggaran kebijakan). Jika verifikator melanggar kebijakannya (mengabaikan permintaan, merespons secara tidak konsisten), peminta memegang tanda tangan asli para saksi σ_i. Tanda tangan ini dapat dipublikasikan sebagai data pendamp-

ing: siapa pun dapat memverifikasi $c_i = h(\sigma_i)$, membuktikan bahwa saksi tersebut hadir. Peminta dapat memublikasikan secara independen—verifikator sudah menandatangani kode tantangan dalam responsnya.

Sifat gertakan. Peminta dapat mengganti sebagian atau seluruh kode tantangan dengan nilai acak. Verifikator tidak dapat membedakan kode asli (didukung oleh otoritas bereputasi tinggi) dari noise. *Ketidakpastian* ini adalah mekanisme penegakannya: setiap permintaan membawa risiko bahwa suatu otoritas yang dihormati sedang mengawasi secara inkognito. Biaya untuk mempertahankan tekanan ini nyaris nol (menghasilkan angka acak), sementara potensi biaya ketidakjujuran bagi verifikator bersifat katastrofik. Perilaku jujur pun terinsentifkan bahkan tanpa kehadiran saksi yang sebenarnya.

Otoritas sebagai saksi. Sebuah Otoritas yang mendukung suatu klaim dapat menggabungkan layanan saksi: "Saya mendukung klaim Anda dan bertindak sebagai saksi inkognito selama verifikasi." Ini adalah model bisnis yang alami—Otoritas sudah memiliki konteksnya. Namun, kedua peran tersebut secara logis independen.

5.5 Prinsip Radikalisme yang Mahal

Tiga saluran biaya bergabung secara bersamaan (Gbr. 6):

Saluran 1: Biaya Iterasi. Setiap penolakan memaksa iterasi baru yang memakan waktu dan sumber daya. Pertumbuhan linear.

Saluran 2: Pembengkakan Dokumen. Setiap iterasi menambahkan respons penuh verifikator ke dokumen klaim. Pertumbuhannya linear, tetapi dengan offset dasar: muatan awal (isi klaim, dukungan otoritas, tanda tangan kriptografis) sudah memiliki ukuran yang tidak sepele B_0. Ukuran total setelah k iterasi: $S(k) = B_0 + k \cdot \Delta$, di mana Δ adalah ukuran respons rata-rata.

Saluran 3: Premi Risiko Verifikator. Risiko bersifat subjektif. Verifikator menilai apakah kebijakan yang dinyatakan DID peminta bertentangan dengan kepentingan komersial, sosial, atau politik verifikator itu sendiri. Premi tersebut dapat meningkat secara eksponensial seiring persepsi jarak dari "ideal" verifikator: $P(d) = \alpha \cdot e^{\beta d}$, di mana d adalah metrik jarak subjektif verifikator. Melampaui batas larangan pribadi, verifikator dapat menolak sepenuhnya.

Yang krusial, ini bukan sensor. Tidak ada klaim yang dilarang. Sistem menetapkan harga risiko (Tabel 1).

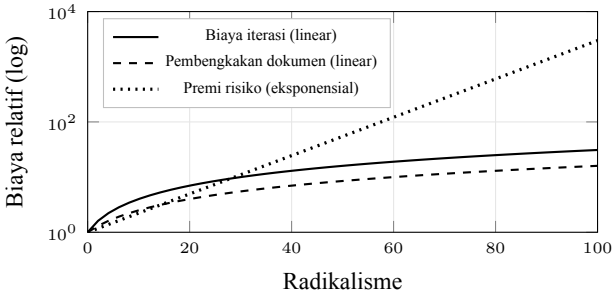

Figure 6: Eskalasi biaya di tiga saluran. Premi risiko mendominasi pada radikalisme tinggi.

Table 1: Perbandingan biaya di berbagai jenis klaim.

Jenis	Iter.	Dok	Biaya	Total
Kredibel	k_{min}	B_0	P_{min}	Rendah
Kontroversial	k_{med}	$B_0 + k\Delta$	$\alpha e^{\beta d}$	Sedang
Radikal	k_{max}	$\gg B_0$	$\gg P_{\text{min}}$	Sangat tinggi
Curang	$\to \infty$	—	—	Tak dapat dipublikasikan

6 Reputasi dan Penilaian Risiko

6.1 Model Akumulasi Reputasi

Reputasi menunjukkan tiga sifat: **akumulasi lambat** (pertumbuhan bertahap melalui perilaku konsisten), **penghancuran cepat** (satu kecurangan dapat menurunkan skor secara katastrofik), dan **evaluasi individual** (setiap pihak yang mengonsumsi dapat menerapkan fungsi agregasinya sendiri).

6.2 Otoritas Bereputasi

Sebuah Otoritas Bereputasi meninjau klaim dan, jika puas, ikut menandatanganinya—mempertaruhkan reputasinya sendiri (Gbr. 7). Asimetri ini disengaja: memperoleh reputasi berjalan lambat (bertahap $+\delta$ per dukungan yang jujur), sementara kehilangannya bersifat katastrofik ($-\Delta \gg \delta$ per dukungan palsu; sebagai ilustrasi, mis., $+2\%$ vs. -70%). Strategi optimalnya selalu menolak klaim yang mencurigakan. Nilai spesifik δ dan Δ merupakan parameter sistem.

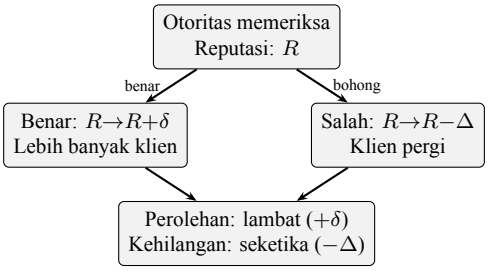

Figure 7: Otoritas Bereputasi—insentif asimetris.

6.3 Reputasi Multidimensi

Reputasi bukanlah skalar melainkan vektor di berbagai dimensi: keandalan finansial, integritas pribadi, kompetensi profesional, keterlibatan sipil, dan lainnya (Gbr. 8). Penyedia evaluasi yang berbeda memproyeksikan vektor ini secara berbeda tergantung konteks—pemberi pinjaman memprioritaskan keandalan finansial, pemberi kerja kompetensi profesional, tetangga perilaku sipil. Tidak ada satu skor reputasi yang "benar" tunggal; hanya perspektif.

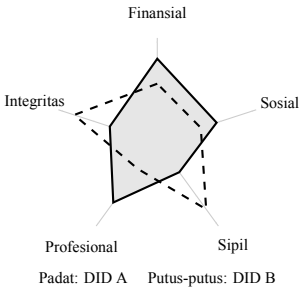

Figure 8: Vektor reputasi multidimensi. DID yang berbeda menunjukkan profil yang berbeda di berbagai dimensi.

6.4 Penilaian Risiko yang Terdemokratisasi

RSN mendemokratisasi penilaian risiko sistematis—sebuah kapabilitas yang saat ini terkonsentrasi pada institusi keuangan tetapi dapat diterapkan jauh melampaui perbankan. Konglomerat industri yang menilai keandalan pemasok, perusahaan asuransi yang menetapkan harga risiko perilaku, uji tuntas untuk merger dan akuisisi, estimasi masa pakai peralatan dalam manufaktur—di mana pun risiko pihak lawan memerlukan penilaian, RSN menyediakan alternatif yang terdesentralisasi dan berbasis pasar. Sebuah pasar layanan interpretasi menerjemahkan data reputasi multidimensi mentah menjadi ringkasan yang dapat ditindaklanjuti, membuat evaluasi pihak lawan dapat diakses oleh peserta mana pun dengan biaya marjinal.

7 Konsensus dan Penyelesaian Sengketa

7.1 Model Keadilan Terdesentralisasi

RSN membingkai ulang keadilan sebagai masalah negosiasi bilateral. Ancaman kerusakan reputasi yang permanen dan dapat diverifikasi merupakan pencegah yang lebih efektif daripada proses hukum yang tidak mampu ditanggung oleh pihak yang dirugikan.

7.2 Konsensus Emergen

Setiap peserta mempertahankan ambang batas kepuasan pribadi. Konsensus agregat jaringan muncul sebagai rata-rata statistik dari ribuan negosiasi bilateral (Gbr. 9). Respons yang jauh di atas konsensus (barbar) mahal untuk dipublikasikan. Respons yang dekat dengan konsensus (proporsional) murah. Konsensus bukanlah sebuah aturan—ia adalah sinyal harga.

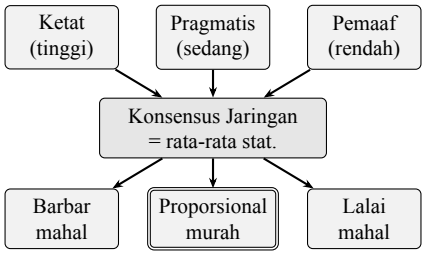

Figure 9: Konsensus emergen dari ambang batas kepuasan individual.

7.3 Kalibrasi Hukuman

Setiap Pemegang DID secara publik menyatakan respons terhadap kategori pelanggaran tertentu. Pernyataan yang terlalu keras atau terlalu lunak secara tidak proporsional menarik sinyal reputasi negatif. Pernyataan yang proporsional diterima tanpa gesekan—sebuah sistem hukuman yang mengalibrasi diri sendiri.

Pernyataan konsensus itu sendiri tunduk pada deteksi kemunafikan: berkomitmen secara deklaratif pada posisi konsensus sambil berperilaku secara tidak konsisten merupakan pelanggaran reputasi yang lebih berat daripada penyimpangan yang mendasarinya, karena hal itu menunjukkan penipuan yang disengaja.

7.4 Pendelegasian

Semua aktivitas dalam sebuah DID—dengan satu pengecualian—dapat didelegasikan ke DID lain. **Peran Subjek—DID yang perilakunya menjadi objek klaim—tidak dapat didelegasikan; ia terikat secara tidak dapat dipindahtangankan kepada pemegang identitas yang dirujuk oleh klaim tersebut.** Peran aktif lainnya—Penerbit, Otoritas, Saksi, Verifikator—dapat dipindahkan ke DID delegasi yang ditunjuk, baik untuk verifikasi, pengajuan klaim, partisipasi konsensus, maupun penyelesaian sengketa. Pendelegasian dapat dicabut kapan saja. Ini memungkinkan spesialisasi (mis., layanan verifikasi profesional) sementara Pemegang mempertahankan kendali dan tanggung jawab tertinggi. Pendelegasian

berlaku di seluruh sistem dan sangat penting untuk skalabilitas.

7.5 Dari Moralitas Individu ke Kontrak Sosial Emergen

Kebijakan yang dinyatakan setiap DID merepresentasikan formalisasi moralitas individu: apa yang dianggap dapat diterima oleh Pemegang, bagaimana mereka merespons perilaku tertentu, apa yang mereka syaratkan dari pihak lawan. Kebijakan-kebijakan ini tidak dipaksakan oleh perancang sistem—ia dipilih oleh setiap peserta dan diekspresikan dalam bentuk yang dapat dibaca mesin.

Formalisasi ini memungkinkan kemunculan tiga tahap. Pertama, moralitas individu dikodekan sebagai **kebijakan**—seperangkat aturan, ambang batas, dan fungsi respons yang dinyatakan yang dijanjikan DID untuk diikuti. Kedua, agregat dari semua kebijakan di seluruh jaringan menghasilkan **etika emergen**—norma-norma yang dapat diamati secara statistik yang tidak dirancang oleh satu peserta pun tetapi muncul dari interaksi ribuan posisi moral individu [9]. Ketiga, etika emergen ini, yang diekspresikan sebagai norma perilaku bersama yang ditegakkan melalui sinyal harga bilateral, membentuk sebuah **kontrak sosial yang terukur**—bukan konstruksi teoretis yang tak seorang pun menandatanganinya [10], melainkan seperangkat aturan yang dapat diamati secara empiris dan didukung oleh perilaku nyata.

Proses ini mencerminkan temuan dari teori moral foundations [11]: moralitas manusia bersifat intuitif, pluralistik, dan bervariasi secara budaya. RSN tidak memerlukan konsensus moral sebagai input; ia menghasilkan konsensus perilaku sebagai output. Kontrak sosial yang dihasilkan tidaklah statis—ia berkembang seiring peserta bergabung, keluar, dan menyesuaikan kebijakan mereka sebagai respons terhadap umpan balik jaringan. Berbeda dengan teori kontrak sosial klasik, kontrak ini dapat dicabut, dapat diamati, dan dapat ditegakkan tanpa seorang penguasa berdaulat.

8 Model Ekonomi

Bagian-bagian sebelumnya menjelaskan sebuah alat—mekanisme verifikasi RSN, struktur biaya, dan konsensus emergen. Bagian ini menjelaskan sebuah metodologi untuk menerapkan alat ini pada transisi fiskal dan tata kelola. Alatnya bersifat serbaguna; metodologi di bawah ini adalah satu aplikasi yang mungkin.

8.1 Struktur Insentif

Reputasi sebagai modal menciptakan insentif langsung untuk perilaku jujur. Dalam operasi normal, peserta membangun reputasi secara alami melalui transaksi sehari-hari dan komitmen yang dipenuhi. Pengeluaran utama adalah untuk klaim *negatif*—mencatat kerugian yang ditimbulkan oleh orang lain. Asimetri ini menginsentifkan perilaku yang berguna dan andal: bersikap jujur tidak menimbulkan biaya tambahan, sementara bersikap merugikan menciptakan jejak terdokumentasi yang akan dibayar orang lain untuk dipertahankan. Kemunafikan—menyatakan aturan tanpa mengikutinya—adalah mode kegagalan yang paling mahal, karena hal itu menunjukkan penipuan yang disengaja.

8.2 Sistem Fiskal Paralel

Tiga komponen memungkinkan tekanan kompetitif: (1) **Pajak Sederhana**—satu tarif proporsional tunggal tanpa pengecualian, awalnya sedikit di bawah tarif efektif yang berlaku; (2) **Registrasi Pengeluaran Elektronik (ESR)**—membalik model EET Ceko sehingga warga negara mengawasi pengeluaran negara; (3) **Alokasi Pajak yang Diarahkan Warga**—dimulai dari beberapa persen pada tahun pertama dan mencapai, setelah satu dekade, di mana pun dari puluhan rendah hingga migrasi penuh ke sistem yang diarahkan warga, tergantung pada laju adopsi. Tempo aktualnya bergantung pada kecepatan munculnya alternatif pasar bebas terhadap layanan negara dan pada kesediaan negara untuk bekerja sama dengan transisi tersebut; fungsi waktu tidak harus linear, dan tidak ada alasan untuk menetapkan batas atas mengenai di mana adopsi pada akhirnya dapat tiba.

9 Jalur Migrasi

Migrasi berlangsung melalui tiga fase (Gbr. 10): **Fase 1: Overlay** (RSN sebagai lapisan informasional, negara adalah satu-satunya penyedia), **Fase 2: Persaingan** (RSN menyediakan alternatif fungsional, penggunaan sistem ganda), dan **Fase 3: Transisi** (RSN mengungguli padanan negara, migrasi sukarela). Transisi ini dapat dibalik pada setiap tahap.

Mekanisme tekanan utama bersifat fiskal: ketika para pembayar pajak bersyarat mencapai "minoritas yang signifikan secara ekonomi X"—sebuah kelompok yang cukup besar sehingga penindasan terhadapnya menyebabkan kerusakan ekonomi yang tidak sepele dan pembangkangan sipil menjadi ancaman

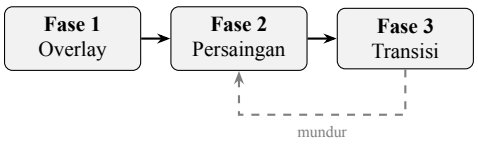

Figure 10: Migrasi tiga fase—dapat dibalik pada setiap tahap.

yang kredibel—negara pun memasuki negosiasi. Untuk ilustrasi, kami menggunakan $X \approx 15\%$ dari PDB, tetapi ambang batas aktualnya bergantung pada ekonomi yang spesifik.

10 Analisis Keamanan

Kami mempertimbangkan lima kategori musuh: pelaku jahat individu, kelompok terorganisir, musuh korporat, musuh tingkat negara, dan musuh tingkat protokol.

Ketahanan Sybil [12]. Membangun reputasi memerlukan interaksi yang berkelanjutan dan dapat diverifikasi. Biaya serangan Sybil yang berhasil berskala linear dengan jumlah identitas palsu dan kuadratik dengan tingkat reputasi target. Mengoperasikan beberapa DID secara paralel dimungkinkan tetapi mahal secara desain—setiap identitas harus mengakumulasikan reputasi secara independen melalui aktivitas yang tulus. Dalam masyarakat bebas biaya ini mencegah penyalahgunaan sembarangan; dalam kediktatoran, DID paralel menjadi alat bertahan hidup yang memungkinkan perlawanan terkompartementalisasi, koordinasi bawah tanah, dan navigasi pasar gelap yang lebih aman.

Pertahanan terhadap kolusi. Pola dukungan timbal balik di antara kelompok tertutup dapat dideteksi melalui analisis grafik sosial. Fungsi agregasi reputasi mendiskon klaim dari sumber yang berkerumun secara rapat.

Musuh tingkat negara. Onion routing, ketiadaan infrastruktur tersentralisasi, dan distribusi peran Verifikator ke seluruh basis peserta memastikan bahwa penindasan memerlukan tindakan yang tidak sebanding dengan manfaat apa pun.

Privasi vs. akuntabilitas. Pseudonimitas—jalan tengah antara anonimitas dan pengungkapan identitas—memungkinkan DID untuk mengakumulasikan reputasi yang bermakna tanpa mengungkapkan identitas dunia nyata Pemegang.

11 Pertimbangan Privasi

Model privasi RSN dibangun di atas pseudonimitas. Pemegang mengendalikan pengungkapan identitas: minimal (pseudonim murni), selektif (kredensial tertentu ditautkan), atau penuh (identitas hukum terkait). Klaim yang dipublikasikan bersifat permanen—sistem mendukung koreksi kontekstual tetapi bukan penghapusan. Seorang Pemegang dapat meninggalkan DID yang telah dikompromikan dan memulai kembali, dengan merelakan reputasi yang telah diakumulasikan.

12 Karya Terkait

Spesifikasi W3C DID Core [2] dan Ceramic Network [8] menyediakan fondasi identitas. EigenTrust [13] mendemonstrasikan agregasi reputasi terdistribusi tanpa otoritas pusat. SBT [3] memperkenalkan token sosial yang tidak dapat dipindahtangankan. RSN berbeda dalam penekanannya pada biaya ekonomi sebagai filter kualitas dan mekanismenya untuk menetapkan harga radikalisme.

DAO [4] dan quadratic voting [5] mendemonstrasikan kelayakan tata kelola terdesentralisasi. RSN menurunkan konsensus dari negosiasi harga bilateral alih-alih pemungutan suara.

Proposal ini menarik dari teori anarko-kapitalis [14, 15] untuk penyediaan layanan swasta tetapi menyimpang dalam dua hal kritis: ia merancang untuk kedengkian dan dorongan pembalasan alih-alih mengasumsikan rasionalitas, dan ia mengusulkan transisi bertahap alih-alih revolusi. Konsep kontrak sosial emergen memiliki pendahulu dalam teori tatanan spontan Hayek [16].

Anarko-agorisme. RSN memiliki banyak kesamaan dengan counter-economics agoris [17]—terutama penekanan pada membangun institusi paralel dan pertukaran sukarela. Namun, agorisme cenderung mengasumsikan kepentingan-diri yang rasional sebagai mekanisme koordinasi yang memadai dan seringkali tidak memiliki jalur migrasi konkret dari struktur negara yang ada. RSN secara eksplisit menyertakan kecenderungan perilaku non-rasional dan menyediakan mekanisme tekanan fiskal untuk transisi bertahap.

Meritokrasi. RSN mungkin merepresentasikan deskripsi fungsional pertama tentang bagaimana meritokrasi [18] dapat muncul sebagai properti sistemik alih-alih sekadar slogan. Sistem meritokratik tradisional gagal karena mereka memerlukan otoritas pusat untuk mendefinisikan dan menegakkan “jasa”. Dalam RSN, jasa muncul dari evaluasi bilateral: mereka yang

memberikan nilai mengakumulasikan reputasi; tidak ada komite yang memutuskan siapa yang memiliki jasa.

Properti sebagai privilese. RSN menyimpang secara fundamental dari perlakuan anarko-kapitalis dan mazhab Austria terhadap hak milik sebagai sesuatu yang alami dan absolut. Dalam kerangka RSN, properti adalah sebuah *privilese*—pengakuan sosial yang, dalam kasus ekstrem, dapat ditarik oleh komunitas ketika seorang peserta secara fundamental melanggar norma bersama (pengkhianatan, penolakan untuk membela komunitas dalam krisis eksistensial, eksploitasi sistematis). Ini bukanlah pengambilalihan oleh negara melainkan penarikan pengakuan sosial oleh jaringan hubungan bilateral.

13 Diskusi dan Keterbatasan

Cold start. Nilai RSN bergantung pada efek jaringan; pengadopsi awal menghadapi nilai yang terbatas sampai partisipasi mencapai ambang batas. Namun, bahkan dari tahap awal, jaringan DID berfungsi sebagai sumber informasi pelengkap yang berguna. Evaluasi reputasi awal dan penilaian otoritas diharapkan berkembang secara bertahap dengan kecanggihan yang meningkat.

Anti-leeching dan kontrol akses. DID target dapat menerapkan biaya berjenjang dan pembatasan akses pada kueri dari DID bereputasi rendah. Ini bukan biner melainkan skala kontinu: semakin sedikit reputasi yang dimiliki suatu DID peminta, semakin sedikit informasi yang diterimanya, semakin lama ia menunggu, dan semakin banyak yang harus dibayarnya. Mekanisme ini menginsentifkan partisipasi yang tulus alih-alih konsumsi pasif.

Ketimpangan akses. Biaya memublikasikan klaim dapat menyaring keluhan yang sah dari peserta yang kurang beruntung secara ekonomi. Mitigasi: setiap peserta secara bersamaan berperan sebagai verifikator potensial (atau mendelegasikan peran ini) dan memperoleh biaya verifikasi. Selama horizon waktu yang cukup, seorang peserta non-radikal seharusnya mendekati netralitas finansial—pendapatan verifikasi kurang lebih mengimbangi biaya publikasi. Ini adalah ekspektasi statistik, bukan jaminan.

Ketimpangan reputasi. Pengadopsi awal mengakumulasikan keunggulan yang dapat menciptakan hambatan bagi pendatang belakangan. Namun, evaluasi reputasi dilakukan oleh penyedia pihak ketiga yang dapat memilih untuk memitigasi keunggulan penggerak pertama melalui algoritma agregasi mereka. Menjadi yang pertama dengan reputasi baik adalah keunggulan ekonomi komparatif yang sah—dan itu memang disengaja.

Pertanyaan terbuka. Fungsi biaya optimal, standar agregasi, tata kelola protokol, dan interaksi dengan data reputasi sintetis yang dihasilkan AI tetap menjadi area untuk pekerjaan di masa depan.

Makalah ini tidak mengklaim bahwa RSN akan menghasilkan hasil yang optimal dalam segala keadaan. Ia mengklaim bahwa RSN merepresentasikan sebuah alternatif yang *layak*—dapat diimplementasikan secara teknis, dapat menopang diri sendiri secara ekonomi, dan kompatibel secara sosial dengan kecenderungan perilaku manusia sebagaimana adanya.

14 Kesimpulan

Makalah ini telah menyajikan Reputation Social Network, sebuah protokol terdesentralisasi yang memungkinkan pertukaran reputasi yang pseudonim dan dapat diverifikasi. Prinsip Radikalisme yang Mahal memastikan bahwa klaim yang curang tersingkir melalui harga tanpa sensor. Jalur migrasi yang diusulkan memungkinkan transisi yang bertahap dan dapat dibalik dari institusi yang ada. Desain ini menyertakan sifat manusia sebagaimana adanya—termasuk kepicikan, kedengkian, dan keinginan akan kepuasan pembalasan—alih-alih menuntut transformasi ideologis. Hasilnya bukanlah utopia melainkan sebuah sistem di mana keadilan dapat diakses, reputasi diperoleh, dan biaya pelanggaran ditanggung oleh pihak yang menyebabkannya.

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.