

Rangkaian Reputasi Ternyahpusat: Suatu Kerangka Kerja untuk Penyusunan Masyarakat Semula Jadi

Pavel Kudrna
Prague, Czechia
Draf v1 — Mac 2026

Abstract

Rasa keadilan—keyakinan bahawa kesalahan diperbetulkan dan jasa diberi ganjaran—merupakan daya perpaduan masyarakat yang paling kuat. Apabila institusi tadbir urus terpusat tidak dapat menyampaikan rasa ini kerana kos menguatkuasakan sesuatu hak melebihi nilai hak itu sendiri, perpaduan sosial menjadi terhakis. Struktur institusi semasa gagal menyelesaikan satu kelas pertikaian yang ketara dengan cara yang secara sistematik sama seperti perancangan pusat gagal memperuntukkan sumber: melalui ketaksimetrian maklumat, gelung maklum balas yang hilang, dan pemisahan pembuat keputusan daripada akibat keputusan mereka. Kertas ini membentangkan Rangkaian Sosial Reputasi (RSN): suatu lapisan komunikasi ternyahpusat, tidak boleh dirasuah, dan tahan penapisan yang dibina di atas Pengecam Ternyahpusat (DID) yang membolehkan peserta samaran menerbit, mengesah, dan mengguna maklumat reputasi tentang tingkah laku dunia nyata. Mekanisme teras bertumpu pada tiga prinsip reka bentuk: (1) struktur kos tidak simetri di mana membaca data reputasi adalah murah tetapi menulis memerlukan usaha yang boleh disahkan; (2) protokol pemilihan pengesah tidak berketentuan berdasarkan pencincangan konsisten yang meletakkan harga pada dakwaan radikal melalui kos lelaran yang meningkat; dan (3) model autoriti reputasi dipacu pasaran di mana pengesah persendirian mempertaruhkan reputasi terkumpul mereka atas ketepatan dakwaan yang mereka sokong. Seni bina yang terhasil menghasilkan meritokrasi muncul tanpa penyelarasan pusat dan membolehkan laluan peralihan beransur-ansur dan boleh diterbalikkan daripada sistem yang ditadbir oleh negara sedia ada.

1 Pengenalan

1.1 Masalah Kepercayaan Terpusat

Tadbir urus moden bertumpu pada satu andaian asas: bahawa institusi terpusat boleh menjadi pengantara kepercayaan antara orang asing pada skala besar. Mahkamah menghakimi pertikaian. Daftar mengesahkan pemilikan. Badan kawal selia menguatkuasakan piawaian. Institusi-institusi ini direka pada era ketika maklumat adalah terhad, komunikasi adalah lambat, dan perwakilan kuasa kepada badan pusat merupakan satu-satunya mekanisme penyelarasan yang boleh dilaksanakan. Walau bagaimanapun, tadbir urus terpusat gagal atas sebab struktur yang sama seperti perancangan pusat: ketaksimetrian maklumat, gelung maklum balas yang hilang, dan pemisahan pembuat keputusan daripada akibat keputusan mereka.

Andaian ini gagal, sebagai contoh, apabila kos pengantaraan institusi melebihi nilai pertikaian. Pertimbangkan seorang penyewa yang mendapati bahawa apartmen sewaan mereka tiada sijil keselamatan elektrik yang dikehendaki oleh undang-undang—suatu keadaan yang menimbulkan bahaya segera kepada nyawa. Hak undang-undang penyewa untuk menarik diri daripada kontrak adalah jelas. Namun kos menguatkuasakan hak itu melalui sistem mahkamah melebihi nilai kewangan deposit dan ganti rugi yang terhutang, walaupun termasuk potensi pampasan berkanun [1]. Tindak balas yang rasional ialah menanggung kerugian dan keluar.

Ini bukan kes tepi yang patologi. Ia merupakan pengalaman lalai bagi satu kelas pertikaian yang ketara di mana kemudaratkan adalah nyata tetapi pertaruhan kewangan jatuh di bawah ambang di mana penguatkuasaan institusi menjadi rasional dari segi ekonomi. Hasilnya ialah suatu sistem yang secara struktur memihak kepada pelaku jahat: mereka yang memudaratkan orang lain dalam jumlah di bawah am-

bang ini boleh bertindak tanpa hukuman, kerana kos menuntut keadilan jatuh ke atas pihak yang dimudaratkan.

Contoh di atas diambil daripada persekitaran undang-undang penulis—sistem undang-undang sivil Czech. Dalam tradisi undang-undang lain—undang-undang lazim berasaskan duluan, undang-undang adat, sistem campuran—keadilan gagal dengan cara yang berbeza dan pada darjah yang berbeza, bergantung pada kekhususan budaya dan prosedur bidang kuasa tersebut. Pembaca kemungkinan akan mengenali contoh setara daripada konteks mereka sendiri. Apa yang universal dari segi struktur ialah coraknya: pertikaian yang nilainya jatuh di bawah ambang penguatkuasaan yang rasional dari segi ekonomi berakhir dengan kerugian ditanggung oleh pihak yang dimudaratkan. RSN tidak menjanjikan keadilan yang sempurna—ia sekadar mengurangkan kelebihan struktur yang dinikmati oleh pelaku jahat apabila penguatkuasaan institusi tidak ekonomik.

1.2 Mengapa Penyelesaian Sedia Ada Tidak Mencukupi

Kerangka kerja Identiti Ternyahpusat (DID) [2] menyediakan mekanisme kriptografi untuk pengurusan identiti berdaulat sendiri tetapi tertumpu terutamanya pada pengesahan identiti tanpa menangani persoalan lebih luas tentang reputasi tingkah laku.

Token Terikat Jiwa (SBT) [3] menangkap wawasan bahawa reputasi tidak boleh dipindah milik tetapi bergantung pada infrastruktur blockchain dengan kekangan keterukuran dan tidak menangani insentif ekonomi yang mengawal kemasukan maklumat. Konsep berkaitan seperti token merit (contohnya, Liberland) berkongsi falsafah yang serupa tetapi kekal terikat pada kerangka bidang kuasa tertentu.

Organisasi Autonomi Ternyahpusat (DAO) [4] melaksanakan tadbir urus melalui kontrak pintar tetapi mengulangi dinamik plutokratik di mana pengaruh adalah berkadar dengan modal. Pengundian kuadratik [5] sebahagiannya mengurangkan hal ini tetapi menghadkan penerimaan praktikal. DAO juga menghadapi *masalah orakel* yang asas: kontrak pintar tidak dapat mengesahkan keadaan dunia nyata dengan boleh dipercayai tanpa sumber luaran yang dipercayai, dan masalah ini tiada penyelesaian umum dalam seni bina blockchain.

Tiada sistem sedia ada yang menggabungkan penyahpusatan, ketahanan penapisan, kesamaran, kos kemasukan yang boleh disahkan, dan konsensus yang muncul.

1.3 Sumbangan

Kertas ini memberikan sumbangan berikut:

1. Takrifan **Rangkaian Sosial Reputasi (RSN)**, suatu protokol ternyahpusat yang memanjangkan kerangka kerja DID untuk menyokong pertukaran reputasi dua hala.
2. Suatu **protokol pemilihan pengesah tidak berketentuan** berdasarkan pencincangan konsisten [6].
3. **Prinsip Radikalisme Mahal**, meletakkan harga pada dakwaan mengikut jarak mereka daripada konsensus rangkaian melalui tiga saluran kos yang berganda.
4. Suatu **model Autoriti Bereputasi** dengan insentif tidak simetri di mana sokongan palsu memakan kos jauh lebih besar secara malapetaka berbanding yuran yang sah.
5. Suatu **laluan peralihan beransur-ansur** melalui infrastruktur fiskal selari.

2 Prinsip Reka Bentuk

Seni bina RSN dikekang oleh lima prinsip reka bentuk yang tidak boleh dirunding.

Kesinambungan dan Evolusi. Sistem ini wujud bersama institusi sedia ada semasa tempoh peralihan yang panjangnya tidak tertentu. Peralihan mesti boleh diterbalikkan pada setiap peringkat.

Kerelaan dan Tanggungjawab. Penyertaan adalah sukarela, tetapi kerelaan digandingkan dengan tanggungjawab: seorang peserta yang mengambil alih kawalan sesuatu fungsi institusi serentak mengambil alih kewajipan yang menyertainya.

Kepelbagaian dan Neutraliti Budaya. Konsensus muncul daripada interaksi dua hala, bukan daripada peraturan yang ditetapkan lebih awal oleh pereka sistem.

Daya Tahan dan Ketahanan Penapisan. Kos menapis rangkaian mesti melebihi kos membiarkannya. Hanya totalitarianisme penuh—dengan kos politik dan ekonomi yang membinasakan—boleh menyekat sistem ini.

Konsensus dan Penguatkuasaan. Sistem ini menggabungkan kecenderungan manusia terhadap kepicikan, dendam, dan kepuasan pembalasan sebagai ciri penanggung beban. Salah laku tidak dilarang; ia diberi harga.

3 Gambaran Keseluruhan Sistem

3.1 Rangkaian Sosial Reputasi

RSN ialah suatu lapisan komunikasi ternyahpusat, rakan ke rakan di mana peserta bertukar maklumat yang boleh disahkan tentang tingkah laku dunia nyata. Sifat penakrifnya ialah: infrastruktur ternyahpusat dan tidak boleh ditapis; penyertaan samaran melalui DID; struktur kos tidak simetri (membaca adalah murah, menulis adalah mahal); kebolehsahan kriptografi; dan **sokongan piawaian**—format boleh dibaca mesin untuk maklumat yang disebarkan melalui rangkaian, untuk perkhidmatan yang ditawarkan oleh autoriti (gubahan dakwaan, sokongan, perkhidmatan saksi), dan untuk format dasar termasuk peraturan untuk menilai reputasi pihak lawan dan menaksir risiko ketidakpadanan dasar (antara tingkah laku yang diisytiharkan dan sebenar).

3.2 Komponen Seni Bina

RSN terdiri daripada empat komponen utama (Raj. 1):

1. **Lapisan DID.** Identiti peserta dengan peraturan yang diisytiharkan, metadata reputasi, dan penghalauan rangkaian.
2. **Protokol Dakwaan.** Format berstruktur untuk menerbitkan pernyataan tentang peristiwa dunia nyata.
3. **Rangkaian Pengesahan.** Protokol ternyahpusat untuk menetapkan pengesah menggunakan pencincangan konsisten.
4. **Lapisan Pengagregatan Reputasi.** Perkhidmatan yang menghasilkan ringkasan reputasi yang boleh dibaca manusia.

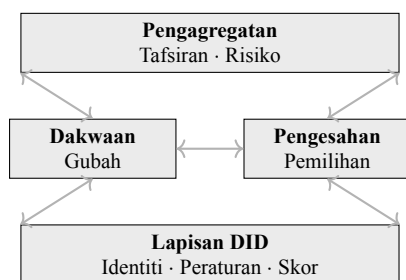


Figure 1: Seni bina empat lapisan RSN.

3.3 Peranan Peserta

Suatu transaksi pengesahan melibatkan sehingga enam peranan DID yang berbeza (Raj. 2): **Pengeluar** (DID_I , mencipta dan menyerahkan dakwaan), **Subjek** (DID_S , DID yang menjadi sub-

jek dakwaan—mungkin bertindih dengan Pengeluar), **Autoriti** (DID_A , menyokong dakwaan dengan yuran; mungkin juga menawarkan perkhidmatan saksi—*pilihan*), **Saksi** ($DID_{W1..n}$, pemantau incognito kejujuran pengesah melalui kod cabaran—*pilihan*), **Pengesah** (DID_V , dipilih secara algoritma untuk menerbitkan dakwaan), dan **RSN** (rangkaihan tempat dakwaan yang disahkan diterbitkan). Mana-mana peranan boleh diwakilkan kepada DID lain (Seksyen 7.4). Suatu Autoriti biasanya menggabungkan sokongan dengan perkhidmatan saksi, tetapi kedua-dua fungsi adalah bebas secara logik.

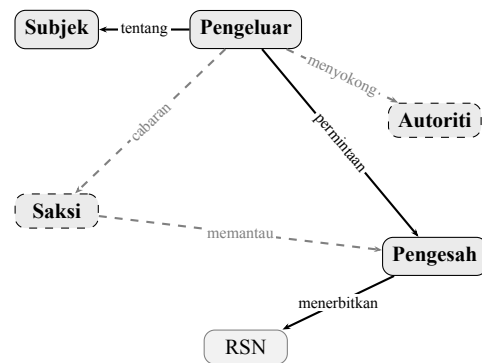


Figure 2: Peranan DID dalam suatu transaksi pengesahan. Putus-putus = pilihan (Autoriti, Saksi).

3.4 Ketidakbolehrasuahan: Empat Daya

Ketidakbolehrasuahan RSN tidak timbul daripada satu mekanisme tunggal tetapi daripada empat daya serentak. Tiada satu pun mencukupi dengan sendirinya; hanya gabungan mereka menjadikan percubaan rasuah tidak rasional dari segi ekonomi.

Sasaran yang tidak dapat diramal. Pengesah bagi setiap dakwaan dipilih secara tidak berketentuan melalui pencincangan konsisten (Seksyen 5.3). Penyerang tidak dapat menyasarkan pengesah tertentu terlebih dahulu untuk rasuah, kerana identiti pengesah adalah fungsi kandungan dakwaan dan lelaran sebelumnya, bukan pilihan pengeluar.

Leveraj reputasi—naik perlahan, turun cepat. Reputasi hanya boleh diperoleh secara beransur-ansur, melalui tingkah laku konsisten yang berterusan. Namun, ia boleh hilang secara malapetaka dalam satu sokongan penipuan (Seksyen 6.2). Ketaksimetrian ini bermakna bertahun-tahun reputasi terkumpul boleh dimusnahkan oleh satu sokongan yang tidak jujur; strategi optimum kekal untuk menolak dakwaan yang mencurigakan.

Janji awam. Setiap Pemegang DID mengisytiharkan dasar mereka secara terbuka—satu set peraturan boleh dibaca mesin yang mereka komit untuk

ikuti. Perbezaan antara pengisytiharan dan tingkah laku sebenar adalah boleh dikesan dan diberi harga sebagai kesalahan reputasi yang lebih teruk daripada pelanggaran asas (Seksyen 7.3). Oleh itu, kemunafikan lebih mahal daripada ketidakjujuran langsung.

Ketaksimetrian kos serangan jejaring. Kos menapis atau menggoyahkan rangkaian bertumbuh secara tidak linear dengan saiz dan ketumpatan rangkaian, sementara kos membiarkannya kekal tetap. Untuk penapisan menjadi berbaloi, seorang pelaku terpusat perlu menggunakannya merentasi seluruh rangkaian—memerlukan langkah yang tidak berkadar dengan sebarang manfaat yang boleh dibayangkan (Seksyen 10).

4 Model Identiti Ternyahpusat

4.1 DID dengan Sifat Khas

RSN memanjangkan spesifikasi W3C DID Core [2] dengan: **Peraturan Diisytiharkan** (komitmen tingkah laku boleh dibaca mesin), **Metadata Reputasi** (skor tingkah laku teragregat), dan **Penghalaan Rangkaian** (get laluan onion boleh ubah yang berasingan daripada kedudukan gelang yang stabil).

4.2 Kitaran Hayat Dakwaan

Suatu Dakwaan melalui enam peringkat (Raj. 3): gubahan, sokongan autoriti pilihan, pemilihan pengesah melalui pencincangan konsisten, keputusan pengesahan (terima atau tolak dengan lelaran), penerbitan, dan kemas kini reputasi untuk semua pihak.

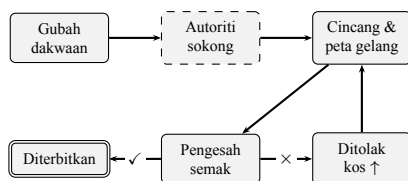


Figure 3: Kitaran hayat dakwaan dengan gelang lelaran.

4.3 Hubungan dengan W3C DID Core

Model identiti RSN merupakan superset sempurna bagi spesifikasi W3C DID Core [2]. Semua DID RSN adalah DID W3C yang sah. Sambungan khusus RSN dikodkan sebagai sifat dokumen DID yang ditakrifkan dalam spesifikasi kaedah DID yang khusus, serasi dengan infrastruktur sedia ada seperti ION [7] dan Ceramic [8].

5 Pengesahan dan Penyebaran Maklumat

5.1 Kos Kemasukan Maklumat

Prinsip ekonomi teras RSN ialah ketaksimetrian antara membaca dan menulis. Membaca data reputasi menghampiri kos sifar bagi peserta yang menjadi sebahagian daripada rangkaian DID dan mempunyai akses yang setara dengan reputasi mereka—pendatang baharu mesti secara beransur-ansur memperoleh akses yang lebih luas (lihat anti-lintah). Menulis—difahami sebagai pewujudan reputasi yang tahan lama ke dalam rangkaian, bukan sebagai satu perbuatan teknikal sekali sahaja—memerlukan pelaburan terkumpul yang boleh disahkan merentasi tiga dimensi: **masa** (bertahun-tahun kehidupan yang dihabiskan pada tingkah laku konsisten, komitmen yang dipenuhi, dan hubungan yang dibina), **tenaga** (usaha yang dilaburkan dalam urus niaga jujur, penjagaan perkongsian, dan kebolehpercayaan jangka panjang), dan **wang** (pelaburan dalam nama sendiri—pembangunan profesional, kualiti kerja seseorang, restitusi atas kemudaratan yang disebabkan). Reputasi tidak boleh dibeli serta-merta—ia adalah hasil pengumpulan sepanjang hayat yang sistem sekadar menjadikannya kelihatan dan boleh dipindahkan merentasi konteks. Kos teknikal sekali sahaja bagi protokol (tanda tangan kriptografi, yuran pengesah) adalah tidak ketara berbanding pelaburan asas ini.

5.2 Graf Sosial dan Kedalaman Kenalan

RSN pada dasarnya ialah suatu rangkaian sosial: setiap DID menambah kenalan (DID lain) yang membenarkan sambungan. Kenalan ini mempunyai kenalan mereka sendiri, dan seterusnya. Carian pengesah algoritma beroperasi dalam kedalaman kenalan berpaut yang boleh dikonfigurasi h (contohnya, $h = 3$: kenalan langsung seseorang, kenalan mereka, dan kenalan bagi kenalan). Seni bina ini tidak memerlukan satu blockchain global tunggal—ia secara semula jadi memihak kepada kemunculan komuniti/kelompok dengan pertindihan ke dalam komuniti lain. Setiap peserta DID mesti mempunyai **dasar** yang diterbitkan—satu set peraturan boleh dibaca mesin yang mengawal bagaimana permintaan masuk dinilai. Pelanggaran dasar direkodkan dalam rangkaian sebagai artifak negatif.

5.3 Pemilihan Pengesah Algoritma

Protokol pengesahan menggunakan pencincangan konsisten [6] (Raj. 4). Pengesahan ialah perkhidmatan berbayar: pengesah beroperasi dengan yuran, mewujudkan pasaran di mana persaingan memacu penetapan harga, kelajuan, dan kebolehpercayaan.

Langkah 1. Dokumen dakwaan digabungkan dengan hasil cincangan lalaran sebelumnya (atau $\emptyset$ pada lalaran pertama) dan dicincang:

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

Algoritma mesti memasukkan *laluhan lengkap* bagi semua permintaan dan respons sebelumnya—bukan sekadar cincangan bagi lalaran sebelumnya. Respons penuh setiap pengesah (penerimaan, penolakan, harga yang disebut, sebab) ditambah pada dokumen yang berkembang, boleh disahkan melalui tandatangan kriptografi pada setiap langkah.

Langkah 2. Cincangan dipetakan kepada N kedudukan pada gelang cincangan konsisten, diagihkan sekata (contohnya, untuk $N = 4$: $+0^\circ, +90^\circ, +180^\circ, +270^\circ$). Daripada setiap kedudukan, carian mengikut pusingan jam memilih DID terdekat sebagai calon pengesah (Raj. 5). N ialah parameter berubah yang mungkin bergantung pada peratusan DID yang aktif buat masa ini, waktu dalam sehari, atau kebolehtindakbalasan rangkaian sejarah.

Langkah 3. Pengesah menerima (menerbitkan, mempertaruhkan reputasi) atau menolak (kembali ke Langkah 1 dengan cincangan penolakan). Apabila sesuatu nod tidak bertindak balas walaupun mengisytiharkan status dalam talian, permintaan seterusnya mesti memasukkan semua respons daripada kesemua N calon pengesah sebelumnya.

Anti-lintah. DID sasaran boleh menetapkan yuran atau sekatan akses untuk pertanyaan daripada DID baharu yang mempunyai sedikit reputasi. Mekanisme berperingkat ini (bukan binari) memaksa pendatang baharu membina reputasi melalui aktiviti tulen sebelum bebas menggunakan data orang lain.

Setiap penolakan menambah respons penuh pengesah (termasuk sebab dan syarat) pada dokumen dakwaan, mengembangkan kandungannya. Daripada dokumen yang dikembangkan, satu cincangan baharu dikira secara tidak berketentuan, memetakan kepada kedudukan gelang yang berbeza dan memilih pengesah yang berbeza. Pendokumenan laluhan penuh adalah wajib—pengeluar tidak dapat meramal atau mempengaruhi pengesah seterusnya. Jika seorang pengesah mengabaikan permintaan walaupun mempunyai dasar diisytihar yang serasi, saksi (jika ada) merekodkan hal

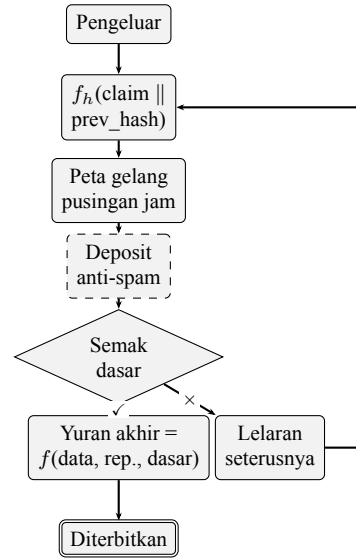


Figure 4: Protokol pemilihan pengesah. Deposit anti-spam adalah pilihan dan mungkin boleh dikembalikan. Yuran akhir dibayar hanya semasa penerimaan.

ini, dan pengeluar boleh melampirkan bukti saksi semasa penerbitan akhir.

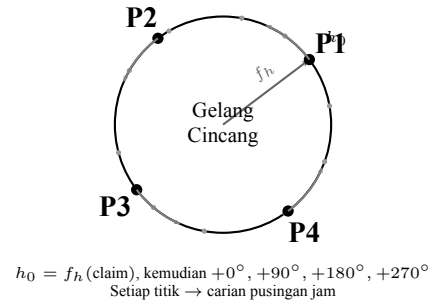


Figure 5: Pemilihan berbilang titik ($N=4$). Cincangan h_0 menetapkan offset; 4 titik diagihkan sekata daripada h_0 .

5.4 Protokol Saksi

Peranan **Saksi** menyediakan kebertanggungjawaban incognito bagi kejujuran pengesah melalui protokol kod cabaran kriptografi:

Langkah W1. Pemohon menandatangani permintaan pengesahan dan menghantarnya kepada N_w saksi—kenalan daripada rangkaian sosial pemohon, atau penyedia perkhidmatan saksi khusus yang beroperasi dengan yuran.

Langkah W2. Setiap saksi w_i menandatangani keseluruhan permintaan yang telah ditandatangani, menyimpan tandatangan asal σ_i , dan mengira kod cabaran $c_i = h(\sigma_i)$. Kod cabaran ditambah pada permintaan.

Langkah W3. Permintaan, kini membawa N_w kod cabaran, dihantar kepada pengesah. Pengesah memerhati kod-kod itu tetapi *tidak dapat menentukan* siapa saksi tersebut atau sama ada kod itu sepadan dengan tandatangan sebenar.

Langkah W4 (pengesah jujur). Jika pengesah bertindak balas mengikut dasar diisytihar mereka, kod cabaran kekal legap. Saksi tidak pernah didedahkan. Tiada data tambahan diterbitkan.

Langkah W5 (pelanggaran dasar). Jika pengesah melanggar dasar mereka (mengabaikan permintaan, bertindak balas secara tidak konsisten), pemohon memegang tandatangan asal saksi σ_i . Ini boleh diterbitkan sebagai data pendamping: sesiapa sahaja boleh mengesahkan $c_i = h(\sigma_i)$, membuktikan saksi hadir. Pemohon boleh menerbitkan secara bebas—pengesah sudah menandatangani kod cabaran dalam respons mereka.

Sifat penipuan. Pemohon boleh menggantikan nilai rawak bagi sebahagian atau kesemua kod cabaran. Pengesah tidak dapat membezakan kod tulen (disokong oleh autoriti bereputasi tinggi) daripada hingar. *Ketidakpastian* ini merupakan mekanisme penguatkuasaan: setiap permintaan membawa risiko bahawa seorang autoriti yang dihormati sedang memerhati secara incognito. Kos mengekalkan tekanan ini adalah hampir sifar (menjana nombor rawak), sementara potensi kos ketidakjujuran bagi pengesah adalah malapetaka. Tingkah laku jujur diberi insentif walaupun tanpa kehadiran saksi sebenar.

Autoriti sebagai saksi. Suatu Autoriti yang menyokong sesuatu dakwaan boleh menggabungkan perkhidmatan saksi: “Saya menyokong dakwaan anda dan berkhidmat sebagai saksi incognito semasa pengesahan.” Ini merupakan model perniagaan yang semula jadi—Autoriti sudah mempunyai konteks. Walau bagaimanapun, kedua-dua peranan adalah bebas secara logik.

5.5 Prinsip Radikalisme Mahal

Tiga saluran kos berganda secara serentak (Raj. 6):

Saluran 1: Kos Lelaran. Setiap penolakan memaksa lelaran baharu yang menggunakan masa dan sumber. Pertumbuhan linear.

Saluran 2: Pengembangan Dokumen. Setiap lelaran menambah respons pengesah penuh pada dokumen dakwaan. Pertumbuhan adalah linear, tetapi dengan ofset asas: muatan awal (kandungan dakwaan, sokongan autoriti, tandatangan kriptografi) sudah mempunyai saiz tidak remeh B_0 . Jumlah saiz selepas k lelaran: $S(k) = B_0 + k \cdot \Delta$, di mana Δ ialah

saiz respons purata.

Saluran 3: Premium Risiko Pengesah. Risiko adalah subjektif. Pengesah menaksir sama ada dasar diisytihar DID yang memohon bercanggah dengan kepentingan komersial, sosial, atau politik pengesah sendiri. Premium mungkin meningkat secara eksponen dengan jarak yang dianggap daripada “ideal” pengesah: $P(d) = \alpha \cdot e^{\beta d}$, di mana d ialah metrik jarak subjektif pengesah. Melangkaui sempadan larangan peribadi, pengesah mungkin menolak sepenuhnya.

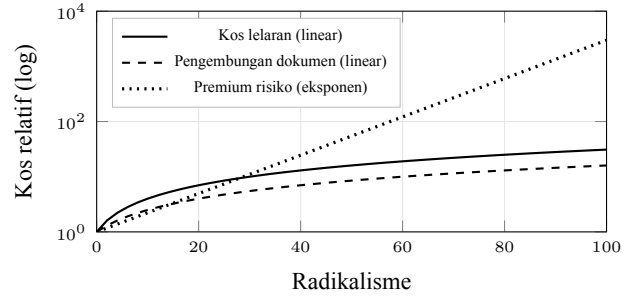


Figure 6: Peningkatan kos merentasi tiga saluran. Premium risiko mendominasi pada radikalisme tinggi.

Yang kritikal, ini bukan penapisan. Tiada dakwaan dilarang. Sistem meletakkan harga pada risiko (Jad. 1).

Table 1: Perbandingan kos merentasi jenis dakwaan.

Jenis	Lelaran	Dok	Yuran	Jumlah
Boleh dipercayai	$k_{\min}$	B_0	$P_{\min}$	Rendah
Kontroversi	k_{med}	$B_0 + k\Delta$	$\alpha e^{\beta d}$	Sederhana
Radikal	$k_{\max}$	$\gg B_0$	$\gg P_{\min}$	Sangat tinggi
Penipuan	$\rightarrow \infty$	—	—	Tidak boleh diterbitkan

6 Penilaian Reputasi dan Risiko

6.1 Model Pengumpulan Reputasi

Reputasi mempamerkan tiga sifat: **pengumpulan perlahan** (pertumbuhan beransur melalui tingkah laku konsisten), **pemusnahan pantas** (satu penipuan boleh mengurangkan skor secara malapetaka), dan **penilaian individu** (setiap pihak yang mengguna boleh menggunakan fungsi pengagregatan mereka sendiri).

6.2 Autoriti Bereputasi

Suatu Autoriti Bereputasi menyemak dakwaan dan, jika berpuas hati, menandatangani bersama—mempertaruhkan reputasinya sendiri (Raj. 7). Ketaksimetrian ini adalah sengaja: memperoleh reputasi adalah perlahan (beransur $+\delta$ setiap sokongan

jujur), sementara kehilangannya adalah malapetaka ($-\Delta \gg \delta$ setiap sokongan palsu; sebagai gambaran, contohnya, $+2\%$ berbanding -70%). Strategi optimum sentiasa untuk menolak dakwaan yang mencurigakan. Nilai khusus δ dan Δ adalah parameter sistem.

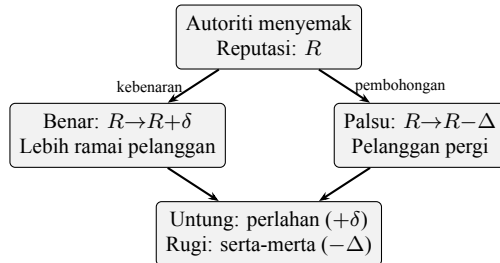


Figure 7: Autoriti Bereputasi—insentif tidak simetri.

6.3 Reputasi Berbilang Dimensi

Reputasi bukan skalar tetapi vektor merentasi berbilang dimensi: kebolehppercayaan kewangan, integriti peribadi, kecekapan profesional, penglibatan sivik, dan lain-lain (Raj. 8). Penyedia penilaian yang berbeza memproyeksi vektor ini secara berbeza bergantung pada konteks—pemberi pinjaman mengutamakan kebolehppercayaan kewangan, majikan mengutamakan kecekapan profesional, jiran mengutamakan tingkah laku sivik. Tiada skor reputasi “betul” yang tunggal; hanya perspektif.

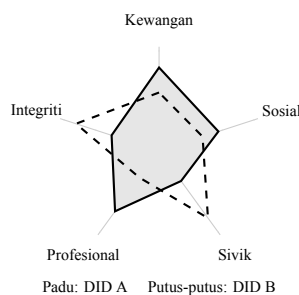


Figure 8: Vektor reputasi berbilang dimensi. DID berbeza mempamerkan profil berbeza merentasi dimensi.

6.4 Penilaian Risiko Terdemokrasi

RSN mendemokrasi penilaian risiko bersistem—suatu keupayaan yang kini tertumpu dalam institusi kewangan tetapi terpakai jauh melangkaui perbankan. Konglomerat industri menaksir kebolehppercayaan pembekal, syarikat insurans meletakkan harga pada risiko tingkah laku, usaha wajar bagi penggabungan dan pengambilalihan, anggaran jangka hayat per-

alatan dalam pembuatan—di mana-mana risiko pihak lawan memerlukan penilaian, RSN menyediakan alternatif ternyahpusat yang dipacu pasaran. Suatu pasaran perkhidmatan tafsiran menterjemah data reputasi berbilang dimensi mentah kepada ringkasan yang boleh ditindaki, menjadikan penilaian pihak lawan boleh diakses oleh mana-mana peserta pada kos sut.

7 Konsensus dan Penyelesaian Pertikaian

7.1 Model Keadilan Ternyahpusat

RSN merangka semula keadilan sebagai masalah rundingan dua hala. Ancaman kerosakan reputasi yang kekal dan boleh disahkan merupakan pencegah yang lebih berkesan daripada prosiding undang-undang yang tidak mampu ditanggung oleh pihak yang dimudaratkan.

7.2 Konsensus Muncul

Setiap peserta mengekalkan ambang kepuasan peribadi. Konsensus agregat rangkaian muncul sebagai purata statistik ribuan rundingan dua hala (Raj. 9). Suatu tindak balas jauh melebihi konsensus (kejam) adalah mahal untuk diterbitkan. Suatu tindak balas hampir dengan konsensus (berkadaran) adalah murah. Konsensus bukan suatu peraturan—ia adalah isyarat harga.

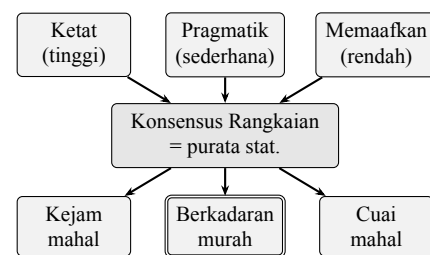


Figure 9: Konsensus muncul daripada ambang kepuasan individu.

7.3 Penentuan Hukuman

Setiap Pemegang DID mengisytiharkan tindak balas secara terbuka terhadap kategori salah laku tertentu. Pengisytiharan yang terlalu keras atau terlalu lembut menarik isyarat reputasi negatif. Pengisytiharan yang berkadaran diterima tanpa geseran—suatu sistem hukuman yang menentukur diri sendiri.

Pengisytiharan konsensus itu sendiri tertakluk kepada pengesanan kemunafikan: berkomit secara pengisytiharan kepada suatu kedudukan konsensus

sambil bertingkah laku secara tidak konsisten merupakan kesalahan reputasi yang lebih teruk daripada sisihan asas, kerana ia menunjukkan penipuan yang disengajakan.

7.4 Perwakilan

Semua aktiviti dalam suatu DID—dengan satu pengecualian—boleh diwakilkan kepada DID lain. **Peranan Subjek—DID yang tingkah lakunya menjadi subjek dakwaan—tidak boleh diwakilkan; ia terikat secara tidak boleh dipindah kepada pemegang identiti yang dirujuk oleh dakwaan.** Peranan aktif yang lain—Pengeluar, Autoriti, Saksi, Pengesah—boleh dipindahkan kepada DID wakil yang ditetapkan, sama ada untuk pengesahan, penyerahan dakwaan, penyertaan konsensus, atau penyelesaian pertikaian. Perwakilan boleh dibatalkan pada bila-bila masa. Ini membolehkan pengkhususan (contohnya, perkhidmatan pengesahan profesional) sementara Pemegang mengekalkan kawalan dan tanggungjawab muktamad. Perwakilan terpakai merentasi seluruh sistem dan penting untuk keterukuran.

7.5 Daripada Moraliti Individu kepada Kontrak Sosial yang Muncul

Dasar diisytihar setiap DID mewakili pemformalan moraliti individu: apa yang dianggap boleh diterima oleh Pemegang, bagaimana mereka bertindak balas terhadap tingkah laku tertentu, apa yang mereka kehendaki daripada pihak lawan. Dasar-dasar ini tidak dikenakan oleh pereka sistem—ia dipilih oleh setiap peserta dan diungkapkan dalam bentuk boleh dibaca mesin.

Pemformalan ini membolehkan kemunculan tiga peringkat. Pertama, moraliti individu dikodkan sebagai **dasar**—satu set peraturan diisytihar, ambang, dan fungsi tindak balas yang DID komit untuk ikuti. Kedua, agregat semua dasar merentasi rangkaian menghasilkan **etika muncul**—norma yang boleh diperhati secara statistik yang tiada seorang peserta pun mereka tetapi yang timbul daripada interaksi ribuan kedudukan moral individu [9]. Ketiga, etika muncul ini, diungkapkan sebagai norma tingkah laku dikongsi yang dikuatkuasakan melalui isyarat harga dua hala, membentuk **kontrak sosial yang boleh diukur**—bukan suatu binaan teori yang tiada sesiapa tandatangani [10], tetapi satu set peraturan yang boleh diperhati secara empirik dan disokong oleh tingkah laku sebenar.

Proses ini mencerminkan penemuan daripada teori asas moral [11]: moraliti manusia adalah intuitif, pluralistik, dan berbeza-beza mengikut budaya. RSN

tidak memerlukan konsensus moral sebagai input; ia menghasilkan konsensus tingkah laku sebagai output. Kontrak sosial yang terhasil tidak statik—ia berkembang apabila peserta menyertai, keluar, dan menyesuaikan dasar mereka sebagai tindak balas kepada maklum balas rangkaian. Tidak seperti teori kontrak sosial klasik, kontrak ini boleh dibatalkan, boleh diperhati, dan boleh dikuatkuasakan tanpa penguasa berdaulat.

8 Model Ekonomi

Seksyen sebelumnya menerangkan suatu alat—mekanisme pengesahan RSN, struktur kos, dan konsensus muncul. Seksyen ini menerangkan suatu metodologi untuk menggunakan alat ini pada peralihan fiskal dan tadbir urus. Alat ini adalah tujuan umum; metodologi di bawah ialah satu aplikasi yang mungkin.

8.1 Struktur Insentif

Reputasi sebagai modal mewujudkan insentif langsung untuk tingkah laku jujur. Dalam operasi biasa, peserta membina reputasi secara semula jadi melalui transaksi harian dan komitmen yang dipenuhi. Perbelanjaan utama adalah pada dakwaan *negatif*—merekodkan kemudaratan yang dilakukan oleh orang lain. Ketaksimetrian ini memberi insentif kepada tingkah laku yang berguna dan boleh dipercayai: bersikap jujur tidak memakan kos tambahan, sementara bersikap memudaratkan mewujudkan jejak berdokumen yang orang lain akan bayar untuk mengekalkannya. Kemunafikan—mengisytiharkan peraturan tanpa mengikutinya—ialah mod kegagalan yang paling mahal, kerana ia menunjukkan penipuan yang disengajakan.

8.2 Sistem Fiskal Selari

Tiga komponen membolehkan tekanan persaingan: (1) **Cukai Ringkas**—suatu kadar berkadaran tunggal tanpa pengecualian, pada mulanya sedikit di bawah kadar berkesan sedia ada; (2) **Pendaftaran Perbelanjaan Elektronik (ESR)**—membalikkan model EET Czech supaya rakyat memantau perbelanjaan negara; (3) **Peruntukan Cukai Diarahkan Rakyat**—bermula pada beberapa peratus dalam tahun pertama dan mencapai, selepas sedekad, di mana-mana antara angka dua digit rendah hingga migrasi penuh kepada sistem diarahkan rakyat, bergantung pada kadar penerimaan. Tempo sebenar bergantung pada kelajuan kemunculan

alternatif pasaran bebas kepada perkhidmatan negara dan pada kesanggupan negara untuk bekerjasama dengan peralihan; fungsi masa tidak semestinya linear, dan tiada sebab untuk menetapkan had atas di mana penerimaan mungkin akhirnya tiba.

9 Laluan Peralihan

Peralihan diteruskan melalui tiga fasa (Raj. 10): **Fasa 1: Lapisan Tindanan** (RSN sebagai lapisan maklumat, negara sebagai penyedia tunggal), **Fasa 2: Persaingan** (RSN menyediakan alternatif berfungsi, penggunaan dwi-sistem), dan **Fasa 3: Peralihan** (RSN mengatasi kesetaraan negara, migrasi sukarela). Peralihan boleh diterbalikkan pada setiap peringkat.

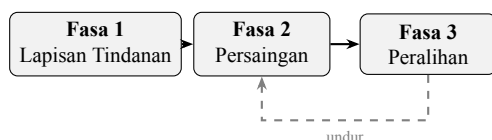


Figure 10: Peralihan tiga fasa—boleh diterbalikkan pada setiap peringkat.

Mekanisme tekanan utama adalah fiskal: apabila pembayar cukai bersyarat mencapai suatu “minoriti signifikan ekonomi X ”—suatu kumpulan yang cukup besar sehingga penindasan terhadapnya menyebabkan kerosakan ekonomi yang tidak remeh dan ketidakpatuhan awam menjadi ancaman yang boleh dipercayai—negara memasuki rundingan. Sebagai gambaran, kami menggunakan $X \approx 15\%$ daripada KDNK, tetapi ambang sebenar bergantung pada ekonomi tertentu.

10 Analisis Keselamatan

Kami mempertimbangkan lima kategori musuh: pelaku jahat individu, kumpulan tersusun, musuh korporat, musuh peringkat negara, dan musuh peringkat protokol.

Ketahanan Sybil [12]. Membina reputasi memerlukan interaksi yang berterusan dan boleh disahkan. Kos serangan Sybil yang berjaya berskala secara linear dengan identiti palsu dan secara kuadratik dengan tahap reputasi sasaran. Mengendalikan berbilang DID secara selari adalah mungkin tetapi mahal secara reka bentuk—setiap identiti mesti mengumpul reputasi secara bebas melalui aktiviti tulen. Dalam masyarakat bebas, kos ini menghalang penyalahgunaan sambil lewa; dalam kediktatoran, DID selari menjadi alat kelangsungan hidup yang membolehkan pe-

nantangan berpetak, penyelarasan bawah tanah, dan pelayaran pasaran gelap yang lebih selamat.

Pertahanan pakatan sulit. Corak sokongan bersama dalam kalangan kumpulan tertutup boleh dikesan melalui analisis graf sosial. Fungsi pengagregatan reputasi mendiskau dakwaan daripada sumber yang berkelompok rapat.

Musuh peringkat negara. Penghalaan onion, ketiadaan infrastruktur terpusat, dan pengagihan peranan Pengesah merentasi asas peserta memastikan bahawa penindasan memerlukan langkah yang tidak berkadar dengan sebarang manfaat.

Privasi berbanding kebertanggungjawaban. Kesamaran—jalan tengah antara kerahsiaan dan pendedahan identiti—membolehkan DID mengumpul reputasi yang bermakna tanpa mendedahkan identiti dunia nyata Pemegang.

11 Pertimbangan Privasi

Model privasi RSN dibina di atas kesamaran. Pemegang mengawal pendedahan identiti: minimum (samaran tulen), terpilih (kelayakan tertentu dipautkan), atau penuh (identiti undang-undang dikaitkan). Dakwaan yang diterbitkan adalah kekal—sistem menyokong pembetulan kontekstual tetapi bukan pemadaman. Seorang Pemegang boleh meninggalkan DID yang terkompromi dan bermula semula, melepaskan reputasi yang terkumpul.

12 Kerja Berkaitan

Spesifikasi W3C DID Core [2] dan Rangkaian Ceramic [8] menyediakan asas identiti. EigenTrust [13] menunjukkan pengagregatan reputasi teragih tanpa autoriti pusat. SBT [3] memperkenalkan token sosial tidak boleh dipindah milik. RSN berbeza dalam penekanannya pada kos ekonomi sebagai penapis kualiti dan mekanismenya untuk meletakkan harga pada radikalisme.

DAO [4] dan pengundian kuadratik [5] menunjukkan kebolehlaksanaan tadbir urus ternyahpusat. RSN memperoleh konsensus daripada rundingan harga dua hala dan bukannya pengundian.

Cadangan ini bertumpu pada teori anarko-kapitalis [14, 15] untuk penyediaan perkhidmatan persendirian tetapi menyimpang dalam dua aspek kritikal: ia mereka bentuk untuk dendam dan dorongan pembalasan dan bukannya mengandaikan kerationalan, dan ia mencadangkan peralihan beransur-ansur dan bukannya revolusi. Konsep kontrak sosial muncul

mempunyai pendahulunya dalam teori susunan spontan Hayek [16].

Anarko-agorisme. RSN berkongsi persamaan yang ketara dengan kontra-ekonomi agoris [17]—terutamanya penekanan pada membina institusi selari dan pertukaran sukarela. Walau bagaimanapun, agorisme cenderung mengandaikan kepentingan diri rasional sebagai mekanisme penyelarasan yang mencukupi dan sering kekurangan laluan peralihan yang konkrit daripada struktur negara sedia ada. RSN secara eksplisit menggabungkan kecenderungan tingkah laku tidak rasional dan menyediakan mekanisme tekanan fiskal untuk peralihan beransur-ansur.

Meritokrasi. RSN mungkin mewakili penerangan berfungsi pertama tentang bagaimana meritokrasi [18] boleh muncul sebagai sifat sistemik dan bukannya slogan. Sistem meritokratik tradisional gagal kerana ia memerlukan autoriti pusat untuk mentakrif dan menguatkuasakan “merit.” Dalam RSN, merit muncul daripada penilaian dua hala: mereka yang menyampaikan nilai mengumpul reputasi; tiada jawatankuasa memutuskan siapa yang mempunyai merit.

Harta sebagai keistimewaan. RSN menyimpang secara asas daripada layanan anarko-kapitalis dan mazhab Austria terhadap hak harta sebagai semula jadi dan mutlak. Dalam kerangka RSN, harta ialah suatu *keistimewaan*—suatu pengiktirafan sosial yang boleh, dalam kes melampau, ditarik balik oleh komuniti apabila seorang peserta melanggar norma dikongsi secara asas (pengkhianatan, keengganan mempertahankan komuniti dalam krisis kewujudan, eksploitasi bersistem). Ini bukan perampasan negara tetapi penarikan balik pengiktirafan sosial oleh rangkaian hubungan dua hala.

13 Perbincangan dan Batasan

Permulaan sejuk. Nilai RSN bergantung pada kesan rangkaian; pengguna awal menghadapi nilai terhad sehingga penyertaan mencapai suatu ambang. Walau bagaimanapun, walaupun dari peringkat awal, rangkaian DID berfungsi sebagai sumber maklumat tambahan yang berguna. Penilaian reputasi awal dan penaksiran autoriti dijangka berkembang secara beransur-ansur dengan kecanggihan yang meningkat.

Anti-lintah dan kawalan akses. DID sasaran boleh mengenakan yuran berperingkat dan sekatan akses ke atas pertanyaan daripada DID reputasi rendah. Ini bukan binari tetapi skala berterusan: semakin sedikit reputasi yang dimiliki oleh suatu DID yang bertanya, semakin sedikit maklumat yang diterima, semakin lama ia menunggu, dan semakin banyak ia memba-

yar. Mekanisme ini memberi insentif kepada penyertaan tulen berbanding penggunaan pasif.

Ketidaksamaan akses. Kos menerbitkan dakwaan mungkin menapis keluar rungutan yang sah daripada peserta yang kurang bernasib baik dari segi ekonomi. Mitigasi: setiap peserta serentak berkhidmat sebagai pengesah berpotensi (atau mewakili peranan ini) dan memperoleh yuran pengesahan. Dalam ufuk masa yang mencukupi, seorang peserta bukan radikal sepatutnya menghampiri kenetralan kewangan—pendapatan pengesahan lebih kurang mengimbangi kos penerbitan. Ini adalah jangkaan statistik, bukan jaminan.

Ketidaksamaan reputasi. Pengguna awal mengumpul kelebihan yang mungkin mewujudkan halangan bagi pendatang lewat. Walau bagaimanapun, penilaian reputasi dilakukan oleh penyedia pihak ketiga yang mungkin memilih untuk mengurangkan kelebihan penggerak pertama melalui algoritma pengagregatan mereka. Menjadi yang pertama dengan reputasi baik ialah suatu kelebihan ekonomi perbandingan yang sah—dan itu adalah secara reka bentuk.

Persoalan terbuka. Fungsi kos optimum, piawaian pengagregatan, tadbir urus protokol, dan interaksi dengan data reputasi sintetik yang dijana AI kekal sebagai bidang untuk kerja masa depan.

Kertas ini tidak mendakwa bahawa RSN akan menghasilkan hasil optimum dalam semua keadaan. Ia mendakwa bahawa RSN mewakili suatu alternatif yang *boleh dilaksanakan*—boleh dilaksanakan secara teknikal, mampan sendiri dari segi ekonomi, dan serasi secara sosial dengan kecenderungan tingkah laku manusia sebagaimana ia sebenarnya wujud.

14 Kesimpulan

Kertas ini telah membentangkan Rangkaian Sosial Reputasi, suatu protokol ternyahpusat yang membolehkan pertukaran reputasi samaran yang boleh disahkan. Prinsip Radikalisme Mahal memastikan bahawa dakwaan penipuan diberi harga terkeluar tanpa penapisan. Laluan peralihan yang dicadangkan membolehkan peralihan beransur-ansur dan boleh diterbalikkan daripada institusi sedia ada. Reka bentuk ini menggabungkan sifat semula jadi manusia sebagaimana adanya—termasuk kepicikan, dendam, dan keinginan untuk kepuasan pembalasan—dan bukannya memerlukan transformasi ideologi. Hasilnya bukan utopia tetapi suatu sistem di mana keadilan boleh diakses, reputasi diperoleh, dan kos salah laku 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.