

Dreifstýrt orðsporsnet: Rammi fyrir náttúrulega samfélagsskipan

Pavel Kudrna
Prague, Czechia
Draft v1 — March 2026

Abstract

Réttlætiskennindin—sannfæringin um að ranglæti verði leiðrétt og verðleikar verðlaunaðir—er sterkasti samloðunarkraftur samfélagsins. Þegar miðstýrðar stofnanir stjórnvalda geta ekki veitt þessa kennd vegna þess að kostnaðurinn við að framfylgja rétti er meiri en verðmæti réttarins sjálfs, veðrast samfélagsleg samloðun. Núverandi stofnanaskipulag nær ekki að leysa umtalsverðan flokk deilna á kerfisbundinn hátt, á sama hátt og miðstýrð áætlanagerð nær ekki að úthluta auðlindum: með ósamhverfum upplýsingum, brostnum endurgjafarrásum og því að ákvörðunartökuaðilar eru slitnir úr tengslum við afleiðingar ákvarðana sinna. Þessi grein kynnir orðspors-samfélagsnet (Reputation Social Network, RSN): dreifstýrt, óspillanlegt og ritskoðunarþolið samskiptalag byggt á dreifstýrðum auðkennum (Decentralized Identifiers, DID) sem gerir gerviauðkenndum þátttakendum kleift að birta, sannreyna og nýta orðsporsupplýsingar um hegðun í raunheimi. Kjarnaþátturinn hvílir á þremur hönnunarreglum: (1) ósamhverfri kostnaðaruppbyggingu þar sem lestur orðsporsgagna er ódýr en ritun krefst sannreynanlegs erfiðis; (2) óákvarðanlegri samskiptareglu um val sannreynenda byggðri á samræmdri tætingu (consistent hashing) sem verðleggur róttækar staðhæfingar með stigvaxandi ítrunarkostnaði; og (3) markaðsdrifnu líkani orðsporsyfirvalds þar sem einkarekin sannreynendur veðja uppsöfnuðu orðspori sínu á nákvæmni þeirra staðhæfinga sem þeir styðja. Sú byggingarlist sem af þessu leiðir framleiðir verðleikaræði án miðstýrðrar samhæfingar og gerir kleift að fara smám saman og afturkræfa leið frá núverandi ríkisreknum kerfum.

1 Inngangur

1.1 Vandamál miðstýrðs trausts

Nú tíma stjórnun hvílir á grundvallarforsendu: að miðstýrðar stofnanir geti miðlað trausti milli ókunn-

gra í stórum stíl. Dómstólar dæma í deilum. Skrár votta eignarhald. Eftirlitsstofnanir framfylgja stöðlum. Þessar stofnanir voru hannaðar á tímum þegar upplýsingar voru af skornum skammti, samskipti hæg og valdaframsal til miðlægrar stofnunar eina raunhæfa samhæfingaraðferðin. Miðstýrð stjórnun bregst hins vegar af sömu byggingarlegu ástæðum og miðstýrð áætlanagerð: ósamhverfum upplýsingum, brostnum endurgjafarrásum og því að ákvörðunartökuaðilar eru slitnir úr tengslum við afleiðingar ákvarðana sinna.

Forsendan bregst til dæmis þegar kostnaðurinn við milligöngu stofnana er meiri en verðmæti deilunnar. Hugsum okkur leigjanda sem uppgötvar að leiguíbúð hans skortir lögbundið rafmagnsöryggisvottorð—ástand sem skapar bráða lífshættu. Lögbundinn réttur leigjandans til að segja sig frá samningnum er ótvíræður. Samt er kostnaðurinn við að framfylgja þeim rétti í gegnum dómskerfið meiri en fjárhagslegt verðmæti tryggingarinnar og skaðabótanna sem honum ber, jafnvel að meðtöldum hugsanlegum lögbundnum bótum [1]. Skynsamlega svarið er að taka á sig tapið og hverfa á braut.

Þetta er ekki afbrigðilegt jaðartilfelli. Þetta er sjálfgefna upplifunin fyrir umtalsverðan flokk deilna þar sem skaðinn er raunverulegur en fjárhagslegu hagsmunirnir falla undir þröskuldinn þar sem framfylgd stofnana verður efnahagslega skynsamleg. Niðurstaðan er kerfi sem byggingarlega hyglir illa innrættum aðilum: þeir sem skaða aðra í magni undir þessum þröskuldi geta athafnað sig án afleiðinga, vegna þess að kostnaðurinn við að leita réttlætis fellur á þann sem skaðaður var.

Dæmið hér að ofan er sótt í lagaumhverfi höfundarins—tékkneska einkaréttarkerfið. Í öðrum réttarhefðum—fordæmisbyggðum almennum rétti (common law), venjurétti, blönduðum kerfum—bregst réttlætið á mismunandi hátt og í mismiklum mæli, allt eftir menningarlegum og málsmeðferðarlegum sérkennum lögsögunnar. Lesendur munu að öllum líkindum kannast við sambærileg dæmi úr eigin samhengi. Það sem er byggingarlega algilt er myn-

strið: deilur þar sem verðmæti fellur undir þröskuld efnahagslega skynsamlegrar framfylgdar enda með því að sá sem skaðaður var tekur á sig tapið. RSN lofar ekki fullkomnu réttlæti—það dregur einfaldlega úr byggingarlega forskotinu sem illa innrættir aðilar njóta þegar framfylgd stofnana er óhagkvæm.

1.2 Hvers vegna núverandi lausnir duga ekki

Rammar dreifstýrðra auðkenna (DID) [2] veita dulkóðunaraðferðir fyrir sjálfstjórnandi auðkennisstýringu en einbeita sér fyrst og fremst að auðkennisstaðfestingu án þess að taka á viðtækari spurningunni um orðspor hegðunar.

Sálbundnir tákn (Soulbound Tokens, SBT) [3] fanga þá innsýn að orðspor sé óframseljanlegt en reiða sig á bálkakeðjuinnviði með skalanleikatakmarkunum og taka ekki á efnahagslegum hvötum sem stýra innskráningu upplýsinga. Skyld hugtök á borð við verðleikatakn (t.d. Liberland) deila svipaðri heimspeki en eru áfram bundin sérstökum lögsagnarrömmum.

Dreifstýrð sjálfstæð samtök (Decentralized Autonomous Organizations, DAO) [4] innleiða stjórnun með snjallsamningum en endurskapa auðræðislega hreyfiafla þar sem áhrif eru í hlutfalli við fjármagn. Ferningsleg atkvæðagreiðsla (quadratic voting) [5] dregur að hluta úr þessu en takmarkar gagnýta upptöku. DAO standa einnig frammi fyrir grundvallarvéftráttarvandann (oracle problem): snjallsamningar geta ekki áreiðanlega sannreynt ástand í raunheimi án trausts ytri upprunaaðila, og þetta vandamál hefur enga almenna lausn innan byggingarlistar bálkakeðja.

Ekkert núverandi kerfi sameinar dreifstýringu, rit-skoðunarþol, gervinafnleynd, sannreynanlegan aðgangskostnað og sjálfsprottna samstöðu.

1.3 Framlög

Þessi grein leggur fram eftirfarandi framlög:

1. Skilgreiningu á **orðspors-samfélagsneti (RSN)**, dreifstýrðri samskiptareglu sem víkkar DID-rammann til að styðja tvíhliða orðsporrsskipti.
2. **Óákvarðanlega samskiptareglu um val sannreynenda** byggða á samræmdri tætingu [6].
3. **Regluna um dýra róttækni** (Expensive Radicalism Principle), sem verðleggur staðhæfingar eftir fjarlægð þeirra frá samstöðu netsins um þrjár uppsafnaðar kostnaðarrásir.
4. **Líkan um orðsporshæft yfirvald** (Reputable Authority) með ósamhverfum hvötum þar sem fölsk stuðningsyfirlýsing kostar stórfellt meira en

lögmaet gjöld.

5. **Leið smám saman umskipta** um samsíða skatkerfisinnviði.

2 Hönnunarreglur

Byggingarlist RSN er bundin fimm ósemjanlegum hönnunarreglum.

Samfella og þróun. Kerfið lifir samhliða núverandi stofnunum á umskiptatímabili af óskilgreindri lengd. Umskiptin verða að vera afturkræf á hverju stigi.

Sjálfviljugni og ábyrgð. Þátttaka er sjálfviljug, en sjálfviljugni fylgir ábyrgð: þátttakandi sem tekur við stjórn stofnanahlutverks tekur um leið á sig meðfylgjandi skyldur.

Fjölbreytni og menningarlegt hlutleysi. Samstaða sprettur af tvíhliða samskiptum, ekki af fyrirframstilltum reglum sem kerfishönnuðir leggja á.

Seigla og ritskoðunarþol. Kostnaðurinn við að rit-skoða netið verður að vera meiri en kostnaðurinn við að umbera það. Aðeins algjört alræði—með gríðarlegum pólitískum og efnahagslegum kostnaði—getur bælt kerfið niður.

Samstaða og framfylgd. Kerfið innlimar mannlega tilhneigingu til smásálar, hefndargirni og hefndarfullnægju sem burðarþætti. Misferli er ekki bannað; það er verðlagt.

3 Yfirlit yfir kerfið

3.1 Orðspors-samfélagsnet

RSN er dreifstýrt jafningjatengt samskiptalag þar sem þátttakendur skiptast á sannreynanlegum upplýsingum um hegðun í raunheimi. Skilgreinandi eiginleikar þess eru: dreifstýrður og óritskoðanlegur innviður; gervinafnleynd þátttöku í gegnum DID; ósamhverf kostnaðaruppbygging (lestur er ódýr, ritun er dýr); dulkóðunarleg sannreynanleiki; og **stuðningur við staðla**—vélalæsileg snið fyrir upplýsingar sem breiðast út um netið, fyrir þjónustu sem yfirvöld bjóða (samsetning staðhæfinga, stuðningsyfirlýsingar, vitnisþjónusta), og fyrir stefnusnið sem iniheldur reglur um mat á orðspori gagnaðila og mat á áhættu af misræmi stefnu (milli yfirlýstrar og raunverulegrar hegðunar).

3.2 Byggingareiningar

RSN samanstendur af fjórum meginþáttum (Mynd 1):

1. **DID-lag.** Auðkenni þátttakenda með yfirlýstum reglum, orðsporslýsigögnum og netbeiningu.
2. **Staðhæfingarregla.** Skipulagt snið til að birta fullyrðingar um raunatburði.
3. **Sannreyningarnet.** Dreifstýrð samskiptaregla til að úthluta sannreynendum með samræmdri tætingu.
4. **Orðsporsamsöfnunarlag.** Þjónustur sem framleiða mannlæsileg orðsporsyfirlit.

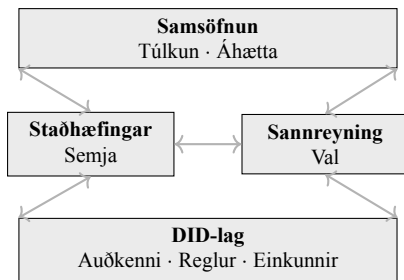


Figure 1: Fjöгурra laga byggingarlist RSN.

3.3 Hlutverk þátttakenda

Sannreyningarviðskipti fela í sér allt að sex aðgreind DID-hlutverk (Mynd 2): **Útgefanda** (DID_I , býr til og leggur fram staðhæfinguna), **Viðfang** (DID_S , það DID sem staðhæfingin fjallar um—getur farið saman við Útgefanda), **Yfirvald** (DID_A , styður staðhæfinguna gegn gjaldi; getur einnig boðið vitnisþjónustu—*valfrjálst*), **Vitni** ($DID_{W_{1..n}}$, huliðsmeðvituð eftirlit með heiðarleika sannreynanda um áskrunarkóða—*valfrjálst*), **Sannreynanda** (DID_V , valinn með reikniriti til að birta staðhæfinguna), og **RSN** (netið þar sem sannreynar staðhæfingar eru birtar). Hvaða hlutverk sem er má framselja til annars DID (Kafli 7.4). Yfirvald tengir oft saman stuðningsyfirlýsingu og vitnisþjónustu, en hlutverkin tvö eru rökrænt óháð.

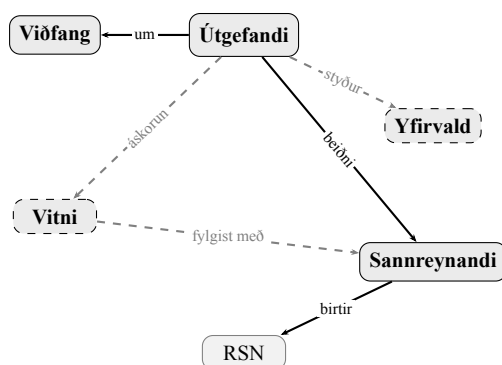


Figure 2: DID-hlutverk í sannreyningarviðskiptum. Punktalínur = valfrjálst (Yfirvald, Vitni).

3.4 Óspillanleiki: fjórir kraftar

Óspillanleiki RSN sprettur ekki af einum þætti heldur af fjórum samhliða kröftum. Enginn er nægilegur einn og sér; aðeins samsetning þeirra gerir tilraun til spillingar efnahagslega óskynsamlega.

Ófyrirsjáanlegt skotmark. Sannreynandinn fyrir hverja staðhæfingu er valinn óákvarðanlega með samræmdri tætingu (Kafli 5.3). Árásaraðili getur ekki fyrirfram beint mótum að tilteknum sannreynanda, vegna þess að auðkenni sannreynandans er fall af efni staðhæfingarinnar og fyrri ítrunum, ekki af vali útgefandans.

Orðsporsvogarafl—hægt upp, hratt niður. Orðspor er aðeins hægt að ávinna smám saman, með viðvarandi samkvæmri hegðun. Það getur hins vegar glatast stórfellt í einni svikafullri stuðningsyfirlýsingu (Kafli 6.2). Þessi ósamhverfa þýðir að ára uppsafnaðs orðspors má eyðileggja með einni óheiðarlegri stuðningsyfirlýsingu; ákjósanlegasta stefnan er áfram að hafna grunsamlegum staðhæfingum.

Opinbert loforð. Sérhver DID-handhafi lýsir opinberlega yfir stefnu sinni—vélalæsilegu setti reglna sem hann skuldbindur sig til að fylgja. Frávik milli yfirlýsingar og raunverulegrar hegðunar er greinanlegt og verðlagt sem orðsporsbrot alvarlegra en undirliggjandi brotið sjálft (Kafli 7.3). Hræsni er því dýrari en bein óheiðarleiki.

Ósamhverfa árásarkostnaðar í möskva. Kostnaðurinn við að ritskoða eða koma netinu úr jafnvægi vex ólínulega með stærð og þéttleika netsins, á meðan kostnaðurinn við að umbera það helst óbreyttur. Til að ritskoðun borgi sig þyrfti miðstýrður aðili að beita henni um allt netið—sem krefðist aðgerða úr öllu hófi við hvaða hugsanlegan ávinning sem er (Kafli 10).

4 Líkan dreifstýrðs auðkennis

4.1 DID með sérstökum eiginleikum

RSN víkkar W3C DID Core forskriftina [2] með: **Yfirlýstum reglum** (vélalæsilegum hegðunarskuldbindingum), **Orðsporslýsigögnum** (samsafnaðri hegðunareinkunn), og **Netbeiningu** (breytanlegri laukhlið aðgreindri frá stöðugri hringstöðu).

4.2 Líftími staðhæfingar

Staðhæfing fer í gegnum sex stig (Mynd 3): samsetningu, valfrjálsa stuðningsyfirlýsingu yfirvalds, val sannreynanda með samræmdri tætingu, sannreyningarákvröðun (samþykki eða höfnun með ítrun),

birtingu, og orðsporsuppfærslu fyrir alla aðila.

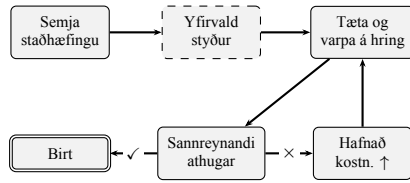


Figure 3: Líftími staðhæfingar með ítrunarlykkju.

4.3 Tengsl við W3C DID Core

Auðkennislíkan RSN er eiginlegt yfirmengi W3C DID Core forskriftarinnar [2]. Öll RSN-DID eru gild W3C-DID. RSN-sértæku útvíkanirnar eru kóðaðar sem eiginleikar DID-skjals sem skilgreindir eru í sérstakri forskrift DID-aðferðar, samhæfðri núverandi innviðum á borð við ION [7] og Ceramic [8].

5 Sannreyning og útbreiðsla upplýsinga

5.1 Kostnaður við innskráningu upplýsinga

Kjarnahagfræðiregla RSN er ósamhverfan milli lesturs og ritunar. Lestur orðsporsgagna nálgast núll jaðarkostnað fyrir þátttakendur sem eru hluti af DID-netinu og hafa aðgang í samræmi við orðspor sitt—nýliðar verða smám saman að ávinna sér viðtækari aðgang (sjá snikjuvörn). Ritun—skilin sem varanleg efnisleg birting orðspors inn í netið, ekki sem einstakur tæknilegur verknaður—krefst sannreynnlegrar uppsafnaðrar fjárfestingar í þremur víddum: **tíma** (æviárum varið í samkvæma hegðun, uppfylltar skuldbindingar og ræktuð tengsl), **orku** (erfiði lagðu í heiðarleg viðskipti, umhyggju fyrir samstarfi og langtímaáreiðanleika), og **peningum** (fjárfestingu í eigin nafni—starfsþróun, gæðum eigin verka, endurgreiðslu fyrir valdinn skaða). Orðspor er ekki hægt að kaupa samstundis—það er afrakstur ævilangrar uppsöfnunar sem kerfið gerir einungis sýnilega og framseljanlega milli samhengja. Einstakur tæknilegur kostnaður samskiptareglunnar (dulkóðunarundirskriftir, gjöld sannreynenda) er hverfandi samanborið við þessa undirliggjandi fjárfestingu.

5.2 Samfélagsgraf og tengsladýpt

RSN er í grunninn samfélagsnet: hvert DID bætir við tengiliðum (öðrum DID) sem leyfa tenginguna. Þessir tengiliðir hafa sína eigin tengiliði, og svo

framvegis. Reikniritsleg leit að sannreynanda starfar innan stillanlegrar dýptar h tengdra tengiliða (t.d. $h = 3$: eigin beinir tengiliðir, tengiliðir þeirra, og tengiliðir tengiliða). Þessi byggingarlist krefst ekki einnar altækrar bálkakeðju—hún hyglir eðlilega tilkomu samfélaga/klasa með skörun inn í önnur samfélög. Sérhver DID-þátttakandi verður að hafa birta **stefnu**—vélalæsilegt sett reglna sem stýrir því hvernig innkomnar beiðnir eru metnar. Stefnubrot eru skráð í netið sem neikvæðir gripir.

5.3 Reikniritslegt val sannreynanda

Sannreyningarreglan notar samræmda tætingu [6] (Mynd 4). Sannreyning er gjaldskyld þjónusta: sannreynendur starfa gegn gjaldi og skapa markað þar sem samkeppni knýr verðlagningu, hraða og áreiðanleika.

Skref 1. Staðhæfingarskjalinu er skeytt saman við tætingarniðurstöðu fyrri ítrunar (eða $\emptyset$ í fyrstu ítrun) og það tætt:

$$\text{staða} = f_h(\text{staðhæfing} \parallel \text{fyrri_tæting}) \quad (1)$$

Reikniritið verður að innihalda *alla slóðina* allra fyrri beiðna og svara—ekki einungis tætingu fyrri ítrunar. Fullt svar hvers sannreynanda (samþykki, höfnun, uppgæfið verð, ástæða) er bætt við vaxandi skjalið, sannreynanlegt með dulkóðunarundirskriftum við hvert skref.

Skref 2. Tætingunni er varpað á N stöður á samræmda tætingarhringnum, jafndreift (t.d. fyrir $N = 4$: $+0^\circ$, $+90^\circ$, $+180^\circ$, $+270^\circ$). Frá hverri stöðu velur réttisælis leit næsta DID sem sannreynandafram-bjóðanda (Mynd 5). N er breytilegur breytustærð sem getur verið háð hlutfalli DID sem eru virk hverju sinni, tíma dags, eða sögulegri svörun netsins.

Skref 3. Sannreynandinn samþykkir (birtir og veðjar orðspori) eða hafnar (og snýr aftur á Skref 1 með höfnunartætingunni). Þegar hnútur svarar ekki þrátt fyrir yfirlýsta nettengingu verður næsta beiðni að innihalda öll svör frá öllum N fyrri sannreynandafram-bjóðendum.

Snikjuvörn. Skotmarks-DID mega setja gjöld eða aðgangstakmarkanir á fyrirspurnir frá nýjum DID með lítið orðspor. Þetta stigskipta fyrirkomulag (ekki tvíundarlegt) þvingar nýliða til að byggja upp orðspor með raunverulegri virkni áður en þeir nýta frjálst gögn annarra.

Hver höfnun bætir fullu svari sannreynandans (þar með talið ástæðum og skilyrðum) við staðhæfingarskjalið og vikkar efni þess. Frá vikkaða skjalinu er ný tæting reiknuð óákvarðanlega, sem varpast á aðra hringstöðu og velur annan sannreynanda. Skráning

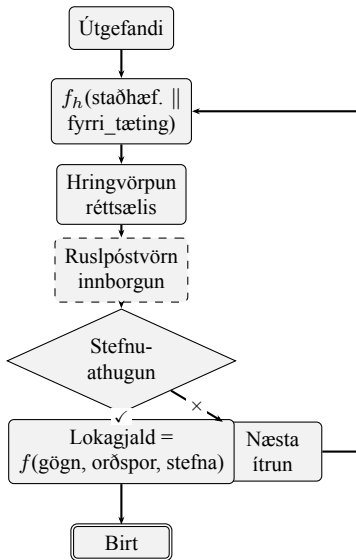


Figure 4: Samskiptaregla um val sannreynanda. Ruslpóstvarnarinnborgun er valfrjál og getur verið endurgreiðanleg. Lokagjald er aðeins greitt við samþykki.

fullrar slóðar er skylda—útgefandinn getur ekki spáð fyrir um eða haft áhrif á næsta sannreynanda. Ef sannreynandi hunsar beiðni þrátt fyrir samhæfa yfirlýsta stefnu, skrá vitni (ef til staðar) það, og útgefandinn má hengja vitnaframburð við lokabirtingu.

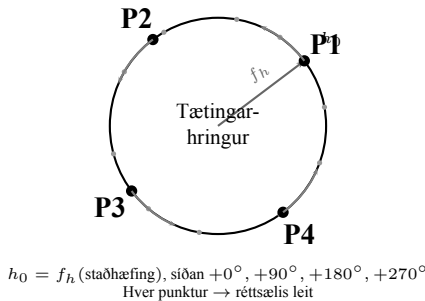


Figure 5: Val með mörgum punktum ($N=4$). Tæting h_0 setur hliðrunina; 4 punktar jafndreifðir frá h_0 .

5.4 Vitnisregla

Vitnishlutverkið veitir huliðsábyrgð fyrir heiðarleika sannreynanda um dulkóðunarreglu áskorunarkóða:

Skref V1. Beiðandinn undirritar sannreyningarbeiðnina og sendir hana til N_w vitna—tengiliða úr samfélagsneti beiðandans, eða sérhæfðra vitnisþjónustuveitenda sem starfa gegn gjaldi.

Skref V2. Hvert vitni w_i undirritar alla undirrituðu beiðnina, heldur upprunalegu undirskriftinni σ_i , og reiknar áskorunarkóða $c_i = h(\sigma_i)$. Áskorunarkóðanum er bætt við beiðnina.

Skref V3. Beiðnin, sem nú ber N_w áskorunarkóða, er send til sannreynandans. Sannreynandinn sér kóðana en *getur ekki ákvarðað* hverjir vitnin eru eða hvort kóðarnir samsvara raunverulegum undirskriftum.

Skref V4 (heiðarlegur sannreynandi). Ef sannreynandinn svarar í samræmi við yfirlýsta stefnu sína, halda áskorunarkóðarnir ógagnsæi sínu. Vitnin eru aldrei afhjúpuð. Engin viðbótargögn eru birt.

Skref V5 (stefnubrot). Ef sannreynandinn brýtur gegn stefnu sinni (hunsar beiðnina, svarar ósamkvæmt), heldur beiðandinn upprunalegum undirskriftum vitnanna σ_i . Þessar má birta sem fylgigögn: hver sem er getur sannreynt $c_i = h(\sigma_i)$, sem sannar að vitnið var viðstatt. Beiðandinn getur birt sjálfstætt—sannreynandinn undirritaði þegar áskorunarkóðana í svari sínu.

Blekkingareiginleikinn. Beiðandinn má skipta út handahófskenndum gildum fyrir suma eða alla áskorunarkóða. Sannreynandinn getur ekki greint ekta kóða (studda af háorðspora yfirlýðum) frá suði. Þessi óvissa er framfylgdarþátturinn: sérhver beiðni ber áhættuna á að virt yfirvald sé að fylgjast með huliðs. Kostnaðurinn við að viðhalda þessum þrýstingi er nálægt núlli (að framleiða handahófstölur), á meðan hugsanlegur kostnaður óheiðarleika fyrir sannreynandann er stórfelldur. Heiðarleg hegðun er hvött jafnvel í fjarveru raunverulegra vitna.

Yfirvald sem vitni. Yfirvald sem styður staðhæfingu má tengja við vitnisþjónustu: „Ég styð staðhæfingu þína og þjóna sem huliðsvitni meðan á sannreyningu stendur.“ Þetta er eðlilegt viðskiptamódel—yfirvaldið hefur þegar samhengið. Hlutverkin tvö eru þó rökrænt óháð.

5.5 Reglan um dýra róttækni

Þrjár kostnaðarrásir aukast samhliða (Mynd 6):

Rás 1: Ítrunarkostnaður. Hver höfnun þvingar fram nýja ítrun sem eyðir tíma og auðlindum. Línulegur vöxtur.

Rás 2: Skjalþensla. Hver ítrun bætir fullu svari sannreynandans við staðhæfingarskjalið. Vöxturinn er línulegur, en með grunnhliðrun: upphaflega álagið (efni staðhæfingar, stuðningsyfirlýsing yfirvalds, dulkóðunarundirskriftir) hefur þegar ekki hverfandi stærð B_0 . Heildarstærð eftir k ítranir: $S(k) = B_0 + k \cdot \Delta$, þar sem Δ er meðalstærð svars.

Rás 3: Áhættuálag sannreynanda. Áhætta er huglæg. Sannreynandinn metur hvort yfirlýstar stefnur beiðnar-DID stangist á við eigin viðskiptalega, samfélagslega eða pólitíska hagsmuni sannreynandans.

Álagið getur aukist veldisvís með skynjaðri fjarlægð frá „hugsjón“ sannreynandans: $P(d) = \alpha \cdot e^{\beta d}$, þar sem d er huglægur fjarlægðarmælikvarði sannreynandans. Handan persónulegra bannmarka getur sannreynandinn hafnað algjörlega.

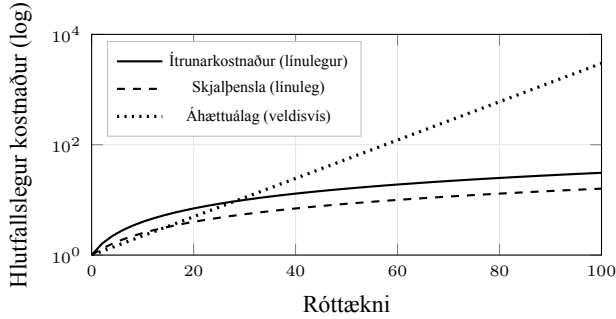


Figure 6: Kostnaðaraukning yfir þrjár rásir. Áhættuálagið ræður ríkjum við mikla róttækni.

Gagnrýnið atriði: þetta er ekki ritskoðun. Engin staðhæfing er bönnuð. Kerfið verðleggur áhættu (Tafla 1).

Table 1: Kostnaðarsamanburður eftir tegundum staðhæfinga.

Tegund	Ítr.	Skjal	Gjald	Alls
Trúverðug	$k_{\min}$	B_0	$P_{\min}$	Lágt
Umdeild	k_{med}	$B_0 + k\Delta$	$\alpha e^{\beta d}$	Miðlungs
Róttæk	$k_{\max}$	$\gg B_0$	$\gg P_{\min}$	Mjög hátt
Svikafull	$\rightarrow \infty$	—	—	Óbirtanleg

6 Orðspor og áhættumat

6.1 Líkan orðsporsuppsöfnunar

Orðspor sýnir þrjá eiginleika: **hæga uppsöfnun** (stígvaxandi vöxt með samkvæmri hegðun), **hraða eyðileggingu** (eitt svik getur lækkað einkunnina stórfellt), og **einstaklingsbundið mat** (hver nýtandi aðili má beita eigin samsöfnunarfalli).

6.2 Orðsporshæf yfirvöld

Orðsporshæft yfirvald yfirfer staðhæfingar og, sé það ánægt, samundirritar þær—veðjar eigin orðspori (Mynd 7). Ósamhverfan er meðvitað hönnuð: að ávinna orðspor er hægt (stígvaxandi $+\delta$ á hverja heiðarlega stuðningsyfirlýsingu), en að tapa því er stórfellt ($-\Delta \gg \delta$ á hverja falsa stuðningsyfirlýsingu; til skýringar, t.d. $+2\%$ á móti -70%). Ákjósanlegasta stefnan er alltaf að hafna grunsam-

legum staðhæfingum. Tiltekin gildi δ og Δ eru kerfisbreytur.

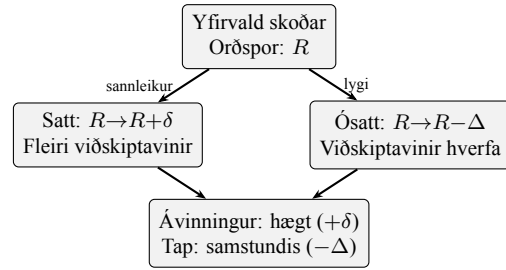


Figure 7: Orðsporshæft yfirvald—ósamhverfir hvatar.

6.3 Fjölvítt orðspor

Orðspor er ekki stærðarstærð heldur vigur yfir margar víddir: fjárhagslegan áreiðanleika, persónulega heilindi, faglega hæfni, borgaralega þátttöku, og fleira (Mynd 8). Ólíkir matsveitendur varpa þessum vigri á mismunandi hátt eftir samhengi—lánveitandi setur fjárhagslegan áreiðanleika í forgang, atvinnurekandi faglega hæfni, nágranni borgaralega hegðun. Það er engin ein „rétt“ orðsporseinkunn; aðeins sjónarhorn.

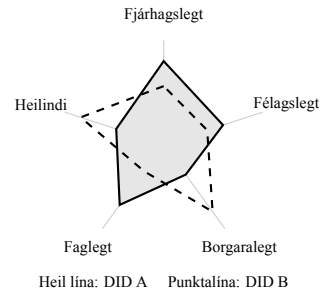


Figure 8: Fjölvíddar orðsporsvigrar. Ólík DID sýna ólík snið yfir víddir.

6.4 Lýðræðisvætt áhættumat

RSN lýðræðisvæðir kerfisbundið áhættumat—getu sem nú er samþjöppuð í fjármálastofnunum en á við langt umfram bankastarfsemi. Iðnaðarsamsteypur sem meta áreiðanleika birgja, tryggingafélög sem verðleggja hegðunaráhættu, áreiðanleikakannanir vegna samruna og yfirtaka, mat á líftíma búnaðar í framleiðslu—hvar sem meta þarf áhættu af gagnaðila veitir RSN dreifstýrðan, markaðsdrifinn valkost. Markaður túlkunarþjónusta þýðir hrá fjölvíddar orðsporsgögn yfir í nýtanleg yfirlit og gerir mat á gagnaðila aðgengilegt hverjum þátttakanda gegn jaðarkostnaði.

7 Samstaða og lausn deilna

7.1 Líkan dreifstýrðs réttlætis

RSN endurskilgreinir réttlæti sem tvíhliða samninga-vandamál. Hótunin um varanlegan, sannreynanlegan orðsporsskaða er áhrifaríkari fæling en dómssál sem sá skaðaði hefur ekki efni á.

7.2 Sjálfsprottin samstaða

Hver þátttakandi viðheldur persónulegum fullnægjuþröskuldi. Heildarsamstaða netsins sprettur fram sem tölfræðilegt meðaltal þúsunda tvíhliða samninga (Mynd 9). Svar langt yfir samstöðunni (villimannlegt) er dýrt að birta. Svar nálægt samstöðunni (í réttu hlutfalli) er ódýrt. Samstaðan er ekki regla—hún er verðmerki.

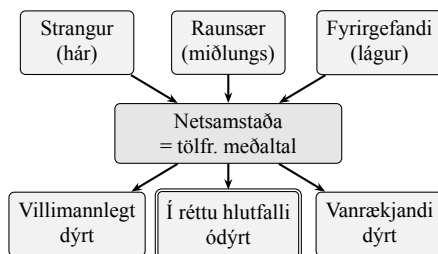


Figure 9: Sjálfsprottin samstaða úr einstaklingsbundnum fullnægjuþröskuldum.

7.3 Kvörðun refsingar

Hver DID-handhafi lýsir opinberlega yfir viðbrögðum við tilteknum flokkum misferlis. Óhóflega harðar eða linar yfirlýsingar draga að sér neikvæð orðsporsmerki. Yfirlýsingar í réttu hlutfalli eru samþykktar án núnings—sjálfkvarðandi refsikerfi.

Samstöðuyfirlýsingar sæta sjálfar hræsnisgreiningu: að skuldbinda sig í orði til samstöðuaftstöðu en haga sér ósamkvæmt er orðsporsbrot alvarlegra en undirliggjandi frávikið, þar sem það sýnir ásetningsblekkingu.

7.4 Framsal

Öll starfsemi innan DID—með einni undantekningu—má framselja til annars DID. **Viðfangshlutverkið—það DID sem hegðun þess staðhæfingin fjallar um—er ekki hægt að framselja; það er óframseljanlega bundið auðkennishandhafanum sem staðhæfingin vísar til.** Hin virku hlutverkin—Útgefandi, Yfirvald, Vitni, Sannreynandi—má framselja til tilnefnds fulltrúa-DID, hvort sem er til sannreyningar, framlagningar staðhæfinga, samstöðupátt-

töku eða lausnar deilna. Framsal er afturkallanlegt hvenær sem er. Þetta gerir kleifa sérhæfingu (t.d. faglega sannreyningaráþjónustu) á meðan handhafinn heldur endanlegri stjórn og ábyrgð. Framsal á við um allt kerfið og er ómissandi fyrir skalanleika.

7.5 Frá einstaklingssiðferði til sjálfsprottins samfélagssáttmála

Yfirlýst stefna hvers DID er formgerving einstaklingssiðferðis: hvað handhafinn telur viðunandi, hvernig hann bregst við tilteknum hegðunum, hvað hann krefst af gagnaðilum. Þessar stefnur eru ekki lagðar á af kerfishönnuði—þær eru valdar af hverjum þátttakanda og settar fram á vélalæsilegu formi.

Þessi formgerving gerir kleift þriggja stiga tilkomu. Í fyrsta lagi er einstaklingssiðferði kóðað sem **stefna**—sett yfirlýstra reglna, þröskulda og viðbragðsfalla sem DID skuldbindur sig til að fylgja. Í öðru lagi framleiðir heildarsafn allra stefna um netið **sjálfsprottið siðferði** (emergent ethics)—tölfræðilega greinanlegar viðmiðanir sem enginn einstakur þátttakandi hannaði en spretta af samspili þúsunda einstaklingsbundinna siðferðilegra afstaðna [9]. Í þriðja lagi mynda þessar sjálfsprottinu siðferðilegu viðmiðanir, settar fram sem sameiginlegar hegðunarviðmiðanir framfylgt um tvíhliða verðmerki, **mælanlegan samfélagssáttmála**—ekki fræðilega hugsmíð sem enginn undirritaði [10], heldur reynslulega greinanlegt sett reglna undirbyggt raunverulegri hegðun.

Þetta ferli speglar niðurstöður úr kenningunni um siðferðilegar undirstöður [11]: mannlegt siðferði er innsæisbundið, fjölhyggjulegt og menningarlega breytilegt. RSN krefst ekki siðferðilegrar samstöðu sem inntaks; það framleiðir hegðunarsamstöðu sem afurð. Sá samfélagssáttmáli sem af þessu leiðir er ekki kyrrstæður—hann þróast eftir því sem þátttakendur bætast við, hverfa á braut og aðlaga stefnur sínar sem svar við endurgjöf netsins. Ólíkt klassískri samfélagssáttmálakenningu er þessi sáttmáli afturkallanlegur, greinanlegur og framfylgjanlegur án fullveldishafa.

8 Efnahagslíkan

Fyrri kaflar lýstu verkfæri—sannreyningaráþttum RSN, kostnaðaruppyggingu og sjálfsprottinni samstöðu. Þessi kafli lýsir aðferðafræði til að beita þessu verkfæri á umskipti í skatt- og stjórnarháttum. Verkfærið er almenns eðlis; aðferðafræðin hér að neðan er ein möguleg beiting.

8.1 Hvatauppbýgging

Orðspor sem fjármagn skapar beina hvata til heiðarlegrar hegðunar. Í venjulegum rekstri byggja þátttakendur upp orðspor eðlilega með daglegum viðskiptum og uppfylltum skuldbindingum. Meginútgjöldin eru á *neikvæðar* staðhæfingar—að skrá skaða sem aðrir valda. Þessi ósamhverfa hvetur til nytsamlegrar, áreiðanlegrar hegðunar: að vera heiðarlegur kostar ekkert aukalega, á meðan það að vera skaðlegur skapar skjalfesta slóð sem aðrir munu greiða fyrir að varðveita. Hræsni—að lýsa yfir reglum án þess að fylgja þeim—er dýrasta bilunarhamurinn, þar sem hún sýnir ásetningsblekkingu.

8.2 Samsíða skattkerfi

Þrír þættir gera samkeppnisþrýsting mögulegan: (1) **Einfaldur skattur**—eitt hlutfallslegt gjald án undantekninga, upphaflega lítillaga undir núverandi raunhlutfalli; (2) **Rafræn skráning útgjalda** (Electronic Spending Registration, ESR)—sem snýr tékkneska EET-likaninu við svo borgarar hafi eftirlit með útgjöldum ríkisins; (3) **Borgarastýrð skattúthlutun**—sem hefst í fáeinum prósentum á fyrsta ári og nær, eftir áratug, hvar sem er frá lágum tveggja stafa tölum upp í fullkomin umskipti yfir í borgarastýrt kerfi, allt eftir hraða upptöku. Raunverulegur hraði er háður því hversu hratt frjálsmarkaðsvalkostir við ríkisþjónustu spretta upp og vilja ríkisins til að vinna með umskiptunum; fall tímans þarf ekki að vera línulegt, og engin ástæða er til að setja efri mörk á hvar upptaka gæti að lokum lent.

9 Umskiptaleið

Umskiptin fara fram í þremur áföngum (Mynd 10): **Áfangi 1: Yfirlag** (RSN sem upplýsingalag, ríkið eini veitandinn), **Áfangi 2: Samkeppni** (RSN veitir virka valkosti, tvíkerfisnotkun), og **Áfangi 3: Umskipti** (RSN skarar fram úr ríkisígildum, sjálfviljug flutningur). Umskiptin eru afturkræf á hverju stigi.

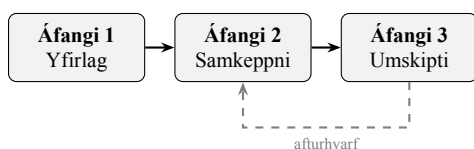


Figure 10: Þriggja áfanga umskipti—afturkræf á hverju stigi.

Meginþrýstipátturinn er skattalegur: þegar skilyrtir skattgreiðendur ná „efnahagslega umtalsverðum min-

nihluta X “—hópi nógu stórum til að kúgun gegn honum valdi ekki-hverfandi efnahagslegu tjóni og borgaraleg óhlýðni verði trúverðug ógn—gengur ríkið til samninga. Til skýringar notum við $X \approx 15\%$ af vergri landsframleiðslu, en raunverulegur þröskuldur er háður hverju hagkerfi fyrir sig.

10 Öryggisgreining

Við ihugum fimm flokka andstæðinga: einstaka illa innrætta aðila, skipulagða hópa, fyrirtækjaandstæðinga, andstæðinga á rikjastigi og andstæðinga á samskiptareglustigi.

Sybil-þol [12]. Að byggja upp orðspor krefst viðvarandi, sannreynanlegra samskipta. Kostnaðurinn við árangursríka Sybil-árás vex línulega með fjölda fál-skra auðkenna og í öðru veldi með markorðsporsstiginu. Að reka mörg DID samhliða er mögulegt en dýrt með ásetningi—hvert auðkenni verður sjálfstætt að safna orðspori með raunverulegri virkni. Í frjálsum samfélögum fælir þessi kostnaður frá lauslegri misnotkun; í einræðisríkjum verða samsíða DID lifunarverkfæri sem gera kleifa hólfaða andspyrnu, neðanjarðarsamhæfingu og öruggari siglingu um svar-tamarkað.

Vörn gegn leynilegu samráði. Mynstur gagnkvæmra stuðningsyfirlýsinga meðal lokaðra hópa eru greinanleg með greiningu samfélagsgrafs. Orðspors-samsöfnunarföll afsláttarreikna staðhæfingar frá þétt klösuðum upprunum.

Andstæðingur á rikjastigi. Laukbeining, fjarvera miðstýrðra innviða og dreifing sannreynandahlutverksins um þátttakendagrunninn tryggja að kúgun krefst aðgerða úr öllu hófi við hvaða ávinning sem er.

Friðhelgi á móti ábyrgð. Gervinafnleynd—millistig milli nafnleyndar og auðkennisupplýsinga—gerir DID kleift að safna merkingarbæru orðspori án þess að opinbera raunverulegt auðkenni handhafans.

11 Friðhelgisatriði

Friðhelgislíkan RSN er byggt á gervinafnleynd. Handhafinn stýrir upplýsingagjöf auðkennis: lágmarks (hreint gervinafn), valkvæð (tiltekin skilríki tengd), eða full (löglegt auðkenni tengt). Birtar staðhæfingar eru varanlegar—kerfið styður samhengislega leiðréttingu en ekki eyðingu. Handhafi má yfirgefa málamiðlað DID og byrja upp á nýtt, og afsala sér uppsöfnuðu orðspori.

12 Skyld verk

W3C DID Core forskriftin [2] og Ceramic Network [8] veita auðkennisgrunninn. EigenTrust [13] sýndi dreifða orðspors-samsöfnun án miðlægs yfirvalds. SBT [3] innleiddu óframseljanleg samfélagstákn. RSN er frábrugðið í áherslu sinni á efnahagslegan kostnað sem gæðasiu og fyrirkomulagi sínu til að verðleggja róttækni.

DAO [4] og ferningsleg atkvæðagreiðsla [5] sýndu fram á fýsileika dreifstýrðrar stjórnunar. RSN leiðir samstöðu af tvíhliða verðsamningum frekar en atkvæðagreiðslu.

Tillagan byggir á anarkó-kapítalískri kenningu [14, 15] um einkaþjónustuveitingu en víkur frá henni í tveimur mikilvægum atriðum: hún hannar fyrir hefndargirni og hefndarhvöt frekar en að gera ráð fyrir skynsemi, og hún leggur til smám saman umskipti frekar en byltingu. Hugtakið um sjálfsprottna samfélagssáttmála á sér forvera í kenningu Hayeks um sjálfsprottna skipan [16].

Anarkó-agórismi. RSN deilir umtalsverðum sameiginlegum grunni með agórískri gagnhagfræði [17]—sérstaklega áherslunni á að byggja upp samsíða stofnanir og sjálfviljug skipti. Agórismi hefur þó tilhneigingu til að gera ráð fyrir skynsamri eigin hagsmunagæslu sem nægilegri samhæfingaraðferð og skortir oft áþreifanlega umskiptaleið frá núverandi ríkisskipulagi. RSN innlimar með berum orðum ó-skynsamlegar hegðunartilhneigingar og veitir skattalegan þrýstipátt fyrir smám saman umskipti.

Verðleikaræði. RSN gæti verið fyrsta virka lýsingin á því hvernig verðleikaræði [18] getur sprottið fram sem kerfiseiginleiki frekar en slagorð. Hefðbundin verðleikakerfi bregðast vegna þess að þau krefjast miðlægs yfirvalds til að skilgreina og framfylgja „verðleikum“. Í RSN sprettur verðleiki fram af tvíhliða mati: þeir sem skila verðmæti safna orðspori; engin nefnd ákveður hver hefur verðleika.

Eign sem forréttindi. RSN víkur í grundvallaratriðum frá anarkó-kapítalískri og austurríska-skólans meðferð eignaréttar sem náttúrulegs og algilds. Í RSN-rammanum er eign *forréttindi*—samfélagsleg viðurkenning sem, í öfgatilfellum, samfélagið getur afturkallað þegar þátttakandi brýtur í grundvallaratriðum gegn sameiginlegum viðmiðunum (svik, neitun um að verja samfélagið í tilvistarkreppu, kerfisbundin arðrán). Þetta er ekki eignaupptaka ríkisins heldur afturköllun samfélagslegrar viðurkenningar af neti tvíhliða tengsla.

13 Umræða og takmarkanir

Kaldræsing. Verðmæti RSN er háð netáhrifum; snemmnótendur standa frammi fyrir takmörkuðu verðmæti þar til þátttaka nær þröskuldi. Samt sem áður, jafnvel frá fyrstu stigum, þjónar DID-netið sem gagnlegur viðbótarupplýsingaruppruni. Búið er við að snemmbúið orðsporsmat og yfirvaldsmat þróist smám saman með aukinni fágun.

Sníkjuvörn og aðgangsstýring. Skotmarks-DID mega leggja stigskipt gjöld og aðgangstakmarkanir á fyrirspurnir frá láorðspora DID. Þetta er ekki tvíundarlegt heldur samfelldur skali: því minna orðspor sem fyrirspyrjandi DID hefur, því minni upplýsingar fær það, því lengur bíður það, og því meira greiðir það. Þetta fyrirkomulag hvetur til raunverulegrar þátttöku umfram óvirkrar neyslu.

Ójöfnuður aðgangs. Kostnaðurinn við að birta staðhæfingar getur síað út lögmætar kvartanir frá efnahagslega illa stæðum þátttakendum. Mildun: sérhver þátttakandi þjónar samtímis sem hugsanlegur sannreynandi (eða framselur það hlutverk) og aflar sannreyningargjalda. Yfir nægilega langt tímabil ætti óróttækur þátttakandi að nálgast fjárhagslegt hlutleysi—sannreyningartekjur jafna nokkurn veginn út birtingarkostnað. Þetta er tölfræðileg vænting, ekki trygging.

Ójöfnuður orðspors. Snemmnótendur safna forskoti sem getur skapað hindranir fyrir siðkomna. Orðsporsmat er þó framkvæmt af þriðju-aðila veitendum sem geta valið að milda forskot snemmnótenda með samsöfnunarreikniritum sínum. Að vera fyrstur með gott orðspor er lögmætt hlutfallslegt efnahagslegt forskot—og það er meðvitað hannað.

Opnar spurningar. Ákjósanleg kostnaðarföll, samsöfnunarstaðlar, stjórnun samskiptareglna og samspil við gervigreindarframleidd tilbúin orðsporsgögn eru áfram svið framtíðarvinnu.

Þessi grein heldur því ekki fram að RSN muni framleiða ákjósanlegar niðurstöður við allar aðstæður. Hún heldur því fram að RSN sé *fýsilegur* valkostur—tæknilega útfæranlegur, efnahagslega sjálfbær og samfélagslega samhæfur mannlegum hegðunartilhneigingum eins og þær eru í raun og veru.

14 Niðurstaða

Þessi grein hefur kynnt orðspors-samfélagsnetið, dreifstýrða samskiptareglu sem gerir kleif gervinafbundin, sannreynanleg orðsporsskipti. Reglan um dýra róttækni tryggir að svikafullar staðhæfingar eru

verðlagðar út án ritskoðunar. Fyrirhuguð umskiptaleið gerir kleif smám saman, afturkræf umskipti frá núverandi stofnunum. Hönnunin innlimar mannlegt eðli eins og það er—þar með talið smásál, hefndargirni og löngun eftir hefndarfullnægju—frekar en að krefjast hugmyndafræðilegrar umbreytingar. Niðurstaðan er ekki útópía heldur kerfi þar sem réttlæti er aðgengilegt, orðspor er áunnið, og kostnaður misferlis er borinn af þeim aðila sem olli því.

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.