

Орталықтандырылмаған бедел желісі: Табиғи қоғамдық ұйымдасудың негіздемесі

Pavel Kudrna
Prague, Czechia
Draft v1 — March 2026

Abstract

Әділдік сезімі—қиянат түзетіледі әрі еңбек марапатталады деген сенім—қоғамның ең күшті ұйыстырушы күші болып табылады. Орталықтандырылған басқару институттары бұл сезімді бере алмаса, өйткені құқықты қорғау шығыны сол құқықтың өз құндылығынан асып кетсе, әлеуметтік ұйысу мүжіле бастайды. Қазіргі институционалдық құрылымдар дауластардың едәуір бөлігін орталық жоспарлаудың ресурстарды бөле алмауымен дәл сол сияқты жүйелі түрде шеше алмайды: ақпараттық асимметрия, кері байланыс тізбектерінің болмауы және шешім қабылдаушылардың өз шешімдерінің салдарынан ажырауы арқылы. Бұл мақала Беделдік әлеуметтік желіні (Reputation Social Network, RSN) ұсынады: бұл—Орталықтандырылмаған идентификаторларға (Decentralized Identifiers, DID) негізделген, орталықтандырылмаған, бұзылмайтын, цензураға төзімді байланыс қабаты, ол жалған атпен қатысатын қатысушыларға нақты дүниедегі мінез-құлық туралы бедел ақпаратын жариялауға, тексеруге және тұтынуға мүмкіндік береді. Негізгі механизм үш жобалау қағидатына сүйенеді: (1) бедел деректерін оқу арзан, ал жазу тексерілетін күш-жігерді талап ететін асимметриялық шығын құрылымы; (2) тұрақты хэштеуге негізделген, радикалды тұжырымдарды өсіп бара жатқан итерация шығыны арқылы бағалайтын детерминалды емес тексеруші таңдау хаттамасы; және (3) жеке тексерушілер өздері мақұлдайтын тұжырымдардың дәлдігіне жинақталған беделін тіккен нарыққа негізделген бедел билігі моделі. Нәтижесінде пайда болатын архитектура орталық үйлестірісін эмерджентті меритократия тудырады және қазіргі мемлекет басқаратын жүйелерден біртіндеп, қайтарылатын көшу жолын мүмкін етеді.

1 Кіріспе

1.1 Орталықтандырылған сенімнің мәселесі

Қазіргі басқару бір іргелі болжамға сүйенеді: орталықтандырылған институттар бейтаныс адамдар арасындағы сенімді ауқымды түрде реттей алады. Соттар дауластарды шешеді. Тіркеу орындары меншікті куәландырады. Реттеуші органдар стандарттарды сақтатады. Бұл институттар ақпарат тапшы, байланыс баяу және билікті орталық органға тапсыру жалғыз мүмкін болатын үйлестіру механизмі болған дәуірде жасалған. Алайда орталықтандырылған басқару орталық жоспарлаумен дәл сол құрылымдық себептерге байланысты сәтсіздікке ұшырайды: ақпараттық асимметрия, кері байланыс тізбектерінің болмауы және шешім қабылдаушылардың өз шешімдерінің салдарынан ажырауы.

Бұл болжам, мысалы, институционалдық делдалдықтың шығыны дауластың құндылығынан асып кеткенде сәтсіздікке ұшырайды. Жалдап алған пәтерінде заң талап ететін электр қауіпсіздігі сертификаты жоқ екенін білген жалдаушыны алайық—бұл өмірге тікелей қауіп төндіретін жағдай. Жалдаушының шарттан бас тарту құқығы даусыз. Алайда сол құқықты сот жүйесі арқылы қорғау шығыны кепіл мен келтірілген залалдың, тіпті ықтимал заңды өтемақыны қосқанда да, ақшалай құнынан асып түседі [1]. Ұтымды жауап—шығынды көтеріп, кету.

Бұл—патологиялық шеткі жағдай емес. Бұл—залал нақты, бірақ ақшалай мөлшер институционалдық қорғау экономикалық тұрғыдан ұтымды болатын шектен төмен түсетін дауластардың едәуір бөлігі үшін әдеттегі тәжірибе. Нәтижесінде жүйе құрылымдық түрде жаман әрекеттерге қолайлы болады: осы шектен төмен көлемде басқаларға зиян келтіргендер жазадан құтылып әрекет ете алады, өйткені әділдік іздеу

шығыны зардап шеккен тарапқа түседі.

Жоғарыдағы мысал автордың құқықтық ортасынан—чех азаматтық құқық жүйесінен—алынған. Басқа құқықтық дәстүрлерде—прецедентке негізделген жалпы құқық, әдет-ғұрып құқығы, аралас жүйелер—әділдік юрисдикцияның мәдени және процедуралық ерекшеліктеріне қарай әртүрлі жолмен және әртүрлі дәрежеде сәтсіздікке ұшырайды. Оқырмандар өз жағдайларынан ұқсас мысалдарды тануы ықтимал. Құрылымдық тұрғыдан әмбебап нәрсе—бұл заңдылық: құндылығы экономикалық тұрғыдан ұтымды қорғау шегінен төмен түсетін дауластар шығынды зардап шеккен тараптың көтеруімен аяқталады. RSN мінсіз әділдікке уәде бермейді—ол тек институционалдық қорғау экономикалық жағынан тиімсіз болғанда жаман әрекет иелерінің ұтатын құрылымдық артықшылығын азайтады.

1.2 Қолданыстағы шешімдер неге жеткіліксіз

Орталықтандырылмаған идентификация (DID) негіздемелері [2] өзін-өзі басқаратын идентификацияны басқарудың криптографиялық механизмдерін ұсынады, бірақ негізінен мінез-құлықтық беделдің кеңірек мәселесін қозғамай, идентификацияны тексеруге бағытталған.

Жанмен байланысқан жетондар (Soulbound Tokens, SBT) [3] беделдің берілмейтіндігі туралы түсінікті қамтиды, бірақ ауқымдау шектеулері бар блокчейн инфрақұрылымына сүйенеді және акпарат енгізуді реттейтін экономикалық ынталандыруларды қозғамайды. Еңбек жетондары (мысалы, *Liberland*) сияқты соған ұқсас тұжырымдамалар ұқсас философияны бөліседі, бірақ нақты юрисдикциялық негіздемелерге байланып қалады.

Орталықтандырылмаған автономды ұйымдар (Decentralized Autonomous Organizations, DAO) [4] басқаруды смарт-келісімшарттар арқылы жүзеге асырады, бірақ ықпал капиталға пропорционал болатын плутократиялық динамиканы қайталайды. Квадраттық дауыс беру [5] мұны ішінара жеңілдетеді, бірақ практикалық қабылдануды шектейді. DAO-лар сондай-ақ іргелі *оракул мәселесіне* тап болады: смарт-келісімшарттар сенімді сыртқы дереккөзсіз нақты дүние жағдайларын сенімді түрде тексере алмайды, ал бұл мәселенің блокчейн архитектурасы аясында жалпы шешімі жоқ.

Қолданыстағы бірде-бір жүйе

орталықсыздандыруды, цензураға төзімділікті, жалған атпен қатысуды, енудің тексерілетін шығынын және эмерджентті консенсусты біріктірмейді.

1.3 Үлестер

Бұл мақала мынадай үлестерді қосады:

1. **Беделдік әлеуметтік желіні (RSN)** анықтау—бұл екіжақты бедел алмасуды қолдау үшін DID негіздемесін кеңейтетін орталықтандырылмаған хаттама.
2. Тұрақты хэштеуге негізделген **детерминалды емес тексеруші таңдау хаттамасы** [6].
3. Тұжырымдарды желі консенсусынан алшақтығына қарай үш өсіп жинақталатын шығын арнасы арқылы бағалайтын **Радикализмнің қымбаттылығы қағидаты**.
4. Жалған мақұлдау заңды алымнан апатты түрде қымбатқа түсетін асимметриялық ынталандырулары бар **Беделді билік моделі**.
5. Қатарлас фискалды инфрақұрылым арқылы **біртіндеп көшу жолы**.

2 Жобалау қағидаттары

RSN архитектурасы бес келіссіз жобалау қағидатымен шектеледі.

Сабақтастық және эволюция. Жүйе өтпелі кезеңде белгісіз ұзақтықта қолданыстағы институттармен қатар өмір сүреді. Өту әр кезеңде қайтарылатын болуы керек.

Еріктілік және жауапкершілік. Қатысу ерікті, бірақ еріктілік жауапкершілікпен ұштасады: институционалдық функцияны басқаруды өз мойнына алған қатысушы бір мезгілде онымен қатар жүретін міндеттемелерді де қабылдайды.

Әртүрлілік және мәдени бейтараптық. Консенсус жүйе жобалаушылары бекіткен алдын ала белгіленген ережелерден емес, екіжақты өзара әрекеттестіктерден пайда болады.

Тұрақтылық және цензураға төзімділік. Желіні цензуралау шығыны оны төзу шығынынан асып түсуі керек. Тек толық тоталитаризм ғана—апатты саяси және экономикалық құн есебінен—жүйені баса алады.

Консенсус және мәжбүрлеу. Жүйе адамдардың ұсақтық, кекшілдік және кек қайтарудан ләззат алу бейімділіктерін негіз болатын мүмкіндіктер ретінде қамтиды. Теріс қылық тыйым салынбайды; ол бағаланады.

3 Жүйеге шолу

3.1 Беделдік әлеуметтік желі

RSN—бұл қатысушылар нақты дүниедегі мінез-құлық туралы тексерілетін ақпаратпен алмасатын орталықтандырылмаған, тең дәрежедегі (peer-to-peer) байланыс қабаты. Оның айқындаушы қасиеттері: орталықтандырылмаған және цензурананбайтын инфрақұрылым; DID арқылы жалған атпен қатысу; асимметриялық шығын құрылымы (оқу арзан, жазу қымбат); криптографиялық тексерілу мүмкіндігі; және **стандарттарды қолдау**—желі арқылы таралатын ақпарат үшін, билік ұсынатын қызметтер үшін (тұжырым құрастыру, мақұлдау, куә қызметі) және саясат форматы, оның ішінде қарсы тараптың беделін бағалау және саясаттың сәйкессіздігі (мәлімделген және нақты мінез-құлық арасындағы) қаупін бағалау ережелерін қоса алғанда, машинамен оқылатын форматтар.

3.2 Архитектуралық құрамдастар

RSN төрт негізгі құрамдастан тұрады (Fig. 1):

1. **DID қабаты.** Мәлімделген ережелері, бедел метадеректері және желілік бағыттауы бар қатысушы идентификациялары.
2. **Тұжырым хаттамасы.** Нақты дүние оқиғалары туралы бекітулерді жариялаудың құрылымды форматы.
3. **Тексеру желісі.** Тұрақты хэштеуді пайдаланып тексерушілерді тағайындаудың орталықтандырылмаған хаттамасы.
4. **Бедел жинақтау қабаты.** Адам оқитын бедел түйіндемелерін өндіретін қызметтер.

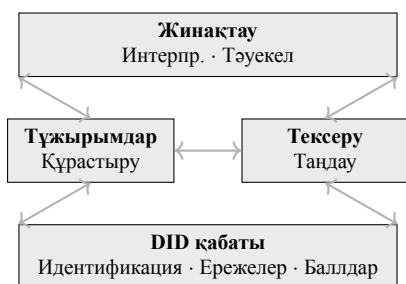


Figure 1: RSN төрт қабатты архитектурасы.

3.3 Қатысушы рөлдері

Тексеру транзакциясына алты бөлек DID рөлі қатысады (Fig. 2): **Шығарушы** (DID_I , тұжырымды жасайды және жібереді), **Субъект**

(DID_S , тұжырым сол туралы болатын DID—Шығарушымен сәйкес келуі мүмкін), **Билік** (DID_A , тұжырымды алым үшін мақұлдайды; куә қызметтерін де ұсынуы мүмкін—*міндетті емес*), **Куә** ($DID_{W_{1..n}}$, сынақ кодтары арқылы тексерушінің адалдығын жасырын бақылаушы—*міндетті емес*), **Тексеруші** (DID_V , тұжырымды жариялау үшін алгоритмдік түрде таңдалады), және **RSN** (тексерілген тұжырымдар жарияланатын желі). Кез келген рөл басқа DID-ке тапсырылуы мүмкін (7.4-бөлім). Билік әдетте мақұлдауды куә қызметтерімен біріктіреді, бірақ бұл екі функция логикалық тұрғыдан тәуелсіз.

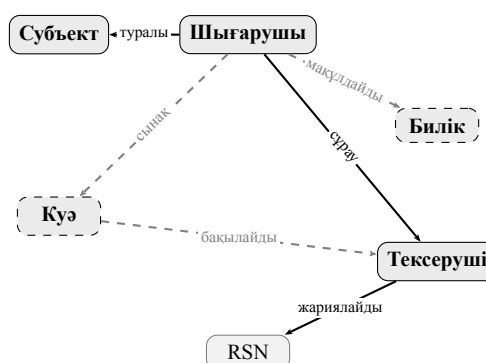


Figure 2: Тексеру транзакциясындағы DID рөлдері. Үзік сызық = міндетті емес (Билік, Куә).

3.4 Бұзылмаушылық: төрт күш

RSN-нің бұзылмаушылығы бір ғана механизмнен емес, төрт қатарлас күштен туындайды. Ешқайсысы жеке-дара жеткіліксіз; тек олардың бірігуі ғана бұзу әрекетін экономикалық тұрғыдан ұтымсыз етеді.

Болжауға келмейтін нысана. Әр тұжырымның тексерушісі тұрақты хэштеу арқылы детерминалды емес түрде таңдалады (5.3-бөлім). Шабуылдаушы белгілі бір тексерушіні пара беру үшін алдын ала нысанаға ала алмайды, өйткені тексерушінің тұлғасы шығарушының таңдауының емес, тұжырымның мазмұны мен алдыңғы итерациялардың функциясы болып табылады.

Беделдік тұтқа—баяу көтеріліп, тез құлайды. Беделді тек біртіндеп, тұрақты дәйекті мінез-құлық арқылы ғана алуға болады. Алайда оны бір алаяқтық мақұлдаумен апатты түрде жоғалтуға болады (6.2-бөлім). Бұл асимметрия жылдар бойы жинақталған беделдің бір адалсыз мақұлдаумен жойылуы мүмкін екенін білдіреді; оңтайлы стратегия күдікті тұжырымдардан бас тарту болып қалады.

Жария уәде. Әр DID иесі өз саясатын—сақтауға

міндеттенген машинамен оқылатын ережелер жиынын—жария түрде мәлімдейді. Мәлімдеме мен нақты мінез-құлық арасындағы алшақтық анықталады және негізгі бұзушылықтан ауырырақ беделдік қылмыс ретінде бағаланады (7.3-бөлім). Сондықтан екіжүзділік тікелей адалсыздықтан қымбатқа түседі.

Топ түріндегі шабуыл шығынының асимметриясы. Желіні цензурау немесе тұрақсыздандыру шығыны желінің көлемі мен тығыздығына қарай сызықты емес түрде өседі, ал оны төзу шығыны тұрақты болып қалады. Цензура өзін ақтауы үшін орталықтандырылған әрекет иесі оны бүкіл желі бойынша қолдануы керек болар еді—бұл кез келген елестетуге болатын пайдаға сәйкессіз шараларды талап етеді (10-бөлім).

4 Орталықтандырылмаған идентификация моделі

4.1 Ерекше қасиеттері бар DID

RSN W3C DID Core спецификациясын [2] мыналармен кеңейтеді: **Мәлімделген ережелер** (машинамен оқылатын мінез-құлықтық міндеттемелер), **Бедел метадеректері** (жинақталған мінез-құлықтық балл) және **Желілік бағыттау** (тұрақты сақина позициясынан бөлек өзгермелі onion шлюз).

4.2 Тұжырымның өмірлік циклі

Тұжырым алты кезеңнен өтеді (Fig. 3): құрастыру, міндетті емес билік мақұлдауы, тұрақты хэштеу арқылы тексеруші таңдау, тексеру шешімі (қабылдау немесе итерациямен бас тарту), жариялау және барлық тараптар үшін бедел жаңарту.

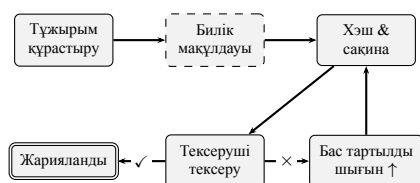


Figure 3: Итерация циклі бар тұжырымның өмірлік циклі.

4.3 W3C DID Core-пен байланысы

RSN-нің идентификация моделі—W3C DID Core спецификациясының [2] нақты асжиыны (super-

set). Барлық RSN DID-тері жарамды W3C DID болып табылады. RSN-ге тән кеңейтулер арнайы DID әдісінің спецификациясында анықталған DID құжатының қасиеттері ретінде кодталады, ION [7] және Ceramic [8] сияқты қолданыстағы инфрақұрылыммен үйлесімді.

5 Ақпаратты тексеру және тарату

5.1 Ақпарат енгізу шығыны

RSN-нің негізгі экономикалық қағидаты—оқу мен жазу арасындағы асимметрия. Бедел деректерін оқу DID желісінің бөлігі болатын және беделіне сәйкес қолжетімділікке ие қатысушылар үшін нөлдік шекті шығынға жақындайды—жаңадан келгендер біртіндеп кеңірек қолжетімділікті еңбегімен алуы керек (leeching-ке қарсы бөлімді қараңыз). Жазу—беделдің бір реттік техникалық әрекет ретінде емес, желіге тұрақты материалдануы ретінде түсінілетіндіктен—үш өлшем бойынша тексерілетін жинақталған салымды талап етеді: **уақыт** (дәйекті мінез-құлыққа, орындалған міндеттемелерге және өсірілген қарым-қатынастарға жұмсалған өмір жылдары), **күш-жігер** (адал іс-әрекетке, серіктестіктерге қамқорлыққа және ұзақ мерзімді сенімділікке салынған еңбек), және **ақша** (өз атына салынған салым—кәсіби даму, өз жұмысының сапасы, келтірілген залалдарды өтеу). Беделді дереу сатып алу мүмкін емес—бұл жүйе тек көрінетін және контексттер арасында берілетін ететін өмір бойы жинақтаудың нәтижесі. Хаттаманың бір реттік техникалық шығындары (криптографиялық қолтаңбалар, тексеруші алымдары) осы негізгі салыммен салыстырғанда болмашы.

5.2 Әлеуметтік граф және байланыс тереңдігі

RSN түбегейлі әлеуметтік желі болып табылады: әр DID байланысқа рұқсат беретін контактілерді (басқа DID-терді) қосады. Бұл контактілердің өз контактілері бар, т.с.с. Алгоритмдік тексеруші іздеу байланысқан контактілердің конфигурацияланатын h тереңдігі шегінде жұмыс істейді (мысалы, $h = 3$: тікелей контактілер, олардың контактілері және контактілердің контактілері). Бұл архитектура бірыңғай ғаламдық блокчейнді талап етпейді—ол басқа қауымдастықтарға қабысатын қауымдастықтардың/кластерлердің

пайда болуын табиғи түрде қолдайды. Әр DID қатысушысында жарияланған **саясат** болуы керек—кіретін сұрауларды қалай бағалауды реттейтін машинамен оқылатын ережелер жиыны. Саясат бұзушылықтары желіде теріс артефактілер ретінде жазылады.

5.3 Алгоритмдік тексеруші таңдау

Тексеру хаттамасы тұрақты хэштеуді [6] қолданады (Fig. 4). Тексеру—ақылы қызмет: тексерушілер алым үшін жұмыс істейді, бұл бәсекелестік бағаны, жылдамдықты және сенімділікті реттейтін нарық тудырады.

1-қадам. Тұжырым құжаты алдыңғы итерацияның хэш нәтижесімен (немесе бірінші итерацияда $\emptyset$) біріктіріледі және хэштеледі:

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

Алгоритм тек алдыңғы итерацияның хэшін ғана емес, барлық алдыңғы сұраулар мен жауаптардың *толық жолын* қамтуы керек. Әр тексерушінің толық жауабы (қабылдау, бас тарту, ұсынылған баға, себеп) өсіп бара жатқан құжатқа қосылады, әр қадамда криптографиялық қолтаңбалар арқылы тексеріледі.

2-қадам. Хэш тұрақты хэш сақинасындағы N позицияға біркелкі бөлінген түрде салынады (мысалы, $N = 4$ үшін: $+0^\circ, +90^\circ, +180^\circ, +270^\circ$). Әр позициядан сағат тілінің бағытымен іздеу ең жақын DID-ті тексеруші үміткер ретінде таңдайды (Fig. 5). N —ағымдағы белсенді DID-тердің пайызына, тәулік уақытына немесе желінің тарихи жауап беру қабілетіне тәуелді болуы мүмкін өзгермелі параметр.

3-қадам. Тексеруші қабылдайды (жариялап, беделін тігеді) немесе бас тартады (бас тарту хэшімен 1-қадамға оралу). Түйін онлайн мәртебесін мәлімдесе де жауап бермегенде, келесі сұрауда барлық N алдыңғы тексеруші үміткерлердің жауаптары болуы керек.

Leeching-ке қарсы. Нысана DID-тері беделі аз жаңа DID-тердің сұраулары үшін алымдар немесе қолжетімділік шектеулерін орната алады. Бұл кезеңдік механизм (екілік емес) жаңадан келгендерді басқалардың деректерін еркін тұтынудан бұрын нақты белсенділік арқылы бедел құруға мәжбүрлейді.

Әр бас тарту тексерушінің толық жауабын (себептер мен шарттарды қоса) тұжырым құжатына қосып, оның мазмұнын кеңейтеді. Кеңейтілген құжаттан жаңа хэш детерминалды

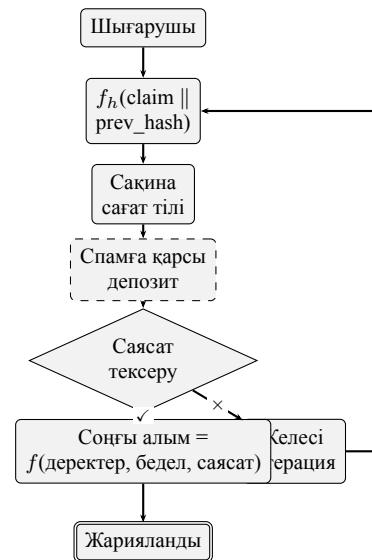


Figure 4: Тексеруші таңдау хаттамасы. Спамға қарсы депозит міндетті емес және қайтарылуы мүмкін. Соңғы алым тек қабылдау кезінде төленеді.

емес түрде есептеліп, басқа сақина позициясына салынады және басқа тексерушіні таңдайды. Толық жолды құжаттау міндетті—шығарушы келесі тексерушіні болжай да, оған ықпал ете де алмайды. Тексеруші үйлесімді мәлімделген саясатқа қарамастан сұрауды елемесе, куәлар (болса) мұны жазады, ал шығарушы соңғы жариялау кезінде куә дәлелдемесін тіркей алады.

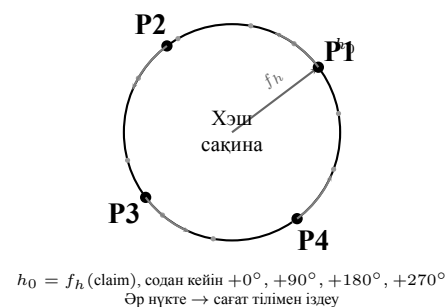


Figure 5: Көп нүктелі таңдау ($N=4$). h_0 хэшы жылжуды белгілейді; h_0 -ден біркелкі бөлінген 4 нүкте.

5.4 Куә хаттамасы

Куә рөлі криптографиялық сынақ-код хаттамасы арқылы тексерушінің адалдығына жасырын жауапкершілікті қамтамасыз етеді:

W1-қадам. Сұрау салушы тексеру сұрауына қол қояды және оны N_w куәға жібереді—сұрау салушының әлеуметтік желісінен

контактілерге немесе алым үшін жұмыс істейтін мамандандырылған куә қызметін ұсынушыларға.

W2-қадам. Әр куә w_i бүкіл қол қойылған сұрауға қол қояды, түпнұсқа қолтаңба σ_i -ды сақтайды және сынақ коды $c_i = h(\sigma_i)$ -ды есептейді. Сынақ коды сұрауға қосылады.

W3-қадам. Енді N_w сынақ кодын алып жүрген сұрау тексерушіге жіберіледі. Тексеруші кодтарды көреді, бірақ куәлардың кім екенін немесе кодтардың нақты қолтаңбаларға сәйкес келетінін *анықтай алмайды*.

W4-қадам (адал тексеруші). Тексеруші өзінің мәлімделген саясатына сәйкес жауап берсе, сынақ кодтары ашылмаған күйінде қалады. Куәлар ешқашан ашылмайды. Ешбір қосымша дерек жарияланбайды.

W5-қадам (саясат бұзушылық). Тексеруші өз саясатын бұзса (сұрауды елемесе, дәйексіз жауап берсе), сұрау салушыда куәлардың түпнұсқа қолтаңбалары σ_i болады. Оларды ілеспе дерек ретінде жариялауға болады: кез келген адам $c_i = h(\sigma_i)$ -ды тексеріп, куәның қатысқанын дәлелдей алады. Сұрау салушы дербес жариялай алады—тексеруші өз жауабында сынақ кодтарына бұрыннан қол қойған.

Блеф қасиеті. Сұрау салушы кейбір немесе барлық сынақ кодтарын кездейсоқ мәндермен алмастыра алады. Тексеруші шынайы кодтарды (беделі жоғары биліктермен қамтамасыз етілген) шуылдан ажырата алмайды. Осы *белгісіздік*—мәжбүрлеу механизмі: әр сұрау беделді биліктің жасырын бақылап отыруы қаупін алып жүреді. Бұл қысымды сақтау шығыны нөлге жуық (кездейсоқ сандар генерациялау), ал тексеруші үшін адалсыздықтың ықтимал шығыны апатты. Адал мінез-құлық нақты куәлар болмаса да ынталандырылады.

Билік куә ретінде. Тұжырымды мақұлдайтын Билік куә қызметтерін біріктіре алады: «Мен сіздің тұжырымыңызды мақұлдаймын және тексеру барысында жасырын куә ретінде қызмет етемін». Бұл—табиғи бизнес-модель—Биліктің контексті бұрыннан бар. Алайда бұл екі рөл логикалық тұрғыдан тәуелсіз.

5.5 Радикализмнің қымбаттылығы қағидаты

Үш шығын арнасы бір мезгілде жинақталады (Fig. 6):

1-арна: Итерация шығыны. Әр бас тарту уақыт пен ресурстарды жұмсайтын жана

итерацияға мәжбүрлейді. Сызықты өсім.

2-арна: Құжаттың ісінуі. Әр итерация тексерушінің толық жауабын тұжырым құжатына қосады. Өсім сызықты, бірақ базалық жылжумен: бастапқы жүктеме (тұжырым мазмұны, билік мақұлдауы, криптографиялық қолтаңбалар) бұрыннан болмашы емес B_0 көлемге ие. k итерациядан кейінгі жалпы көлем: $S(k) = B_0 + k \cdot \Delta$, мұндағы Δ —орташа жауап көлемі.

3-арна: Тексерушінің тәуекел үстемесі. Тәуекел субъективті. Тексеруші сұрау салушы DID-тің мәлімделген саясаты өзінің коммерциялық, әлеуметтік немесе саяси мүдделерімен қайшы келе ме, соны бағалайды. Үстеме тексерушінің «идеалынан» қабылданатын алшақтыққа қарай экспоненциалды түрде өсуі мүмкін: $P(d) = \alpha \cdot e^{\beta d}$, мұндағы d —тексерушінің субъективті алшақтық өлшемі. Жеке рұқсат етілмейтін шектен тыс болса, тексеруші толықтай бас тартуы мүмкін.

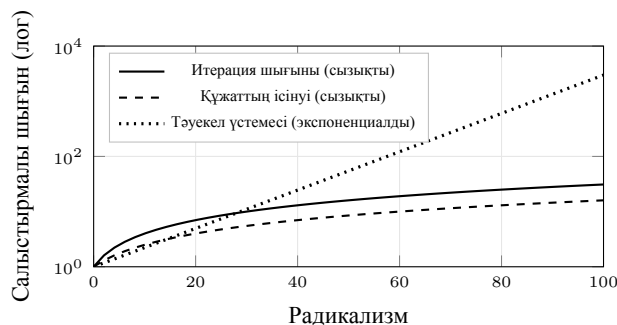


Figure 6: Үш арна бойынша шығынның өсуі. Тәуекел үстемесі жоғары радикализмде басым болады.

Ең бастысы, бұл—цензура емес. Ешбір тұжырым тыйым салынбайды. Жүйе тәуекелді бағалайды (Table 1).

Table 1: Тұжырым түрлері бойынша шығын салыстыруы.

Түрі	Итер.	Құж.	Алым	Барлығы
Сенімді	$k_{\min}$	B_0	$P_{\min}$	Төмен
Даулы	k_{med}	$B_0 + k\Delta$	$\alpha e^{\beta d}$	Орташа
Радикалды	$k_{\max}$	$\gg B_0$	$\gg P_{\min}$	Өте жоғары
Алаяқтық	$\rightarrow \infty$	—	—	Жарияланбайтын

6 Бедел мен тәуекелді бағалау

6.1 Бедел жинақтау моделі

Беделдің үш қасиеті бар: **баяу жинақталу** (дәйекті мінез-құлық арқылы біртіндеп өсу), **жылдам жойылу** (бір алаяқтық баллды апатты түрде төмендете алады) және **жеке бағалау** (әр тұтынушы тарап өз жинақтау функциясын қолдана алады).

6.2 Беделді биліктер

Беделді билік тұжырымдарды қарайды және қанағаттанса, оларға бірге қол қояды—өз беделін тігеді (Fig. 7). Асимметрия әдейі жобаланған: бедел алу баяу (әр адал мақұлдауда біртіндеп $+\delta$), ал оны жоғалту апатты (әр жалған мақұлдауда $-\Delta \gg \delta$; мысал ретінде $+2\%$ -ке қарсы -70%). Оңтайлы стратегия—әрдайым күдікті тұжырымдардан бас тарту. δ мен Δ -ның нақты мәндері—жүйе параметрлері.

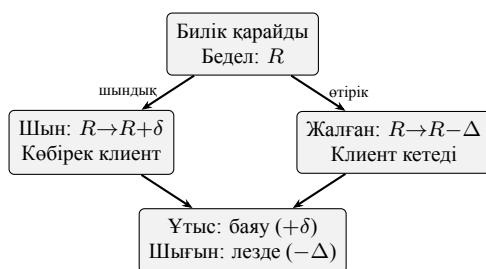


Figure 7: Беделді билік—асимметриялық ынталандырулар.

6.3 Көпөлшемді бедел

Бедел—скаляр емес, бірнеше өлшем бойынша вектор: қаржылық сенімділік, жеке адалдық, кәсіби құзыреттілік, азаматтық белсенділік және басқалар (Fig. 8). Әртүрлі бағалау провайдерлері бұл векторды контекстке қарай әртүрлі жобалайды—несие беруші қаржылық сенімділікке, жұмыс беруші кәсіби құзыреттілікке, көрші азаматтық мінез-құлыққа басымдық береді. Бірыңғай «дұрыс» бедел баллы жоқ; тек көзқарастар бар.

6.4 Демократияландырылған тәуекелді бағалау

RSN жүйелі тәуекелді бағалауды демократияландырады—қазіргі уақытта

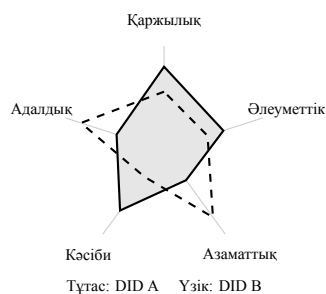


Figure 8: Көпөлшемді бедел векторлары. Әртүрлі DID-тер өлшемдер бойынша әртүрлі профиль көрсетеді.

қаржы институттарында шоғырланған, бірақ банк ісінен әлдеқайда кеңірек қолданылатын мүмкіндік. Жеткізушінің сенімділігін бағалайтын өнеркәсіптік конгломераттар, мінез-құлықтық тәуекелді бағалайтын сақтандыру компаниялары, бірігулер мен жұтулар үшін дью-дилидженс, өндірістегі жабдықтың қызмет ету мерзімін бағалау—қарсы тарап тәуекелін бағалау қажет болатын кез келген жерде RSN орталықтандырылмаған, нарыққа негізделген балама ұсынады. Интерпретация қызметтерінің нарығы шикі көпөлшемді бедел деректерін іс-әрекетке жарамды түйіндемелерге аударып, қарсы тарапты бағалауды кез келген қатысушыға шекті шығынмен қолжетімді етеді.

7 Консенсус және дауды шешу

7.1 Орталықтандырылмаған әділдік моделі

RSN әділдікті екіжақты келіссөз мәселесі ретінде қайта тұжырымдайды. Тұрақты, тексерілетін бедел зақымының қаупі зардап шеккен тарап төлей алмайтын сот процесіне қарағанда тиімдірек тежеуші болып табылады.

7.2 Эмерджентті консенсус

Әр қатысушы жеке қанағаттану шегін ұстайды. Желінің жиынтық консенсусы мыңдаған екіжақты келіссөздердің статистикалық орташасы ретінде пайда болады (Fig. 9). Консенсустан әлдеқайда жоғары жауап (тағылық) жариялау қымбат. Консенсусқа жақын жауап (пропорционал) арзан. Консенсус—ереже емес, ол баға сигналы.

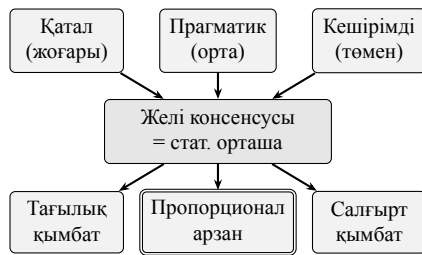


Figure 9: Жеке қанағаттану шектерінен пайда болатын эмерджентті консенсус.

7.3 Жазаны калибрлеу

Әр DID иесі нақты теріс қылық санаттарына жауаптарды жария түрде мәлімдейді. Пропорционалдылықтан тыс қатал немесе жұмсақ мәлімдемелер теріс бедел сигналдарын тартады. Пропорционалды мәлімдемелер үйкеліссіз қабылданады—өзін-өзі калибрлейтін жаза жүйесі.

Консенсус мәлімдемелерінің өздері екіжүзділікті анықтауға жатады: консенсус ұстанымына мәлімдемелік түрде міндеттеніп, дәйексіз әрекет ету негізгі ауытқудан ауырырақ беделдік қылмыс болып табылады, өйткені ол әдейі алдауды көрсетеді.

7.4 Тапсыру (делегация)

DID шеңберіндегі барлық әрекеттер—бір ерекшелікпен—басқа DID-ке тапсырылуы мүмкін. **Субъект рөлі—мінез-құлық туралы тұжырым айтылатын DID—тапсырыла алмайды; ол тұжырым сілтейтін идентификация иесіне берілмейтін түрде байланады.** Басқа белсенді рөлдер—Шығарушы, Билік, Куә, Тексеруші—тексеру, тұжырым жіберу, консенсусқа қатысу немесе дауды шешу үшін тағайындалған делегат DID-ке берілуі мүмкін. Тапсыру кез келген уақытта қайтарылады. Бұл мамандандыруды мүмкін етеді (мысалы, кәсіби тексеру қызметтері), сонымен қатар иесі түпкі бақылау мен жауапкершілікті сақтайды. Тапсыру бүкіл жүйе бойынша қолданылады және ауқымдау үшін маңызды.

7.5 Жеке моральдан эмерджентті қоғамдық келісімшартқа

Әр DID-тің мәлімделген саясаты жеке моральдың формализациясын білдіреді: иесі нені қолайлы деп санайды, нақты мінез-құлыққа қалай жауап береді, қарсы тараптан нені талап етеді. Бұл саясаттарды жүйе жобалаушысы таңылмайды—оларды әр қатысушы таңдайды және машинамен

оқылатын түрде білдіреді.

Бұл формализация үш кезеңдік эмерджентцияны мүмкін етеді. Біріншіден, жеке мораль **саясат** ретінде кодталады—DID сақтауға міндеттенген мәлімделген ережелер, шектер және жауап функцияларының жиыны. Екіншіден, желі бойынша барлық саясаттардың жиынтығы **эмерджентті этиканы** тудырады—ешбір жеке қатысушы жобаламаған, бірақ мыңдаған жеке моральдық ұстанымдардың өзара әрекеттестігінен пайда болатын статистикалық түрде байқалатын нормалар [9]. Үшіншіден, екіжақты баға сигналдары арқылы мәжбүрленетін ортақ мінез-құлықтық нормалар ретінде білдірілетін бұл эмерджентті этика **өлшенетін қоғамдық келісімшартты** құрайды—ешкім қол қоймаған теориялық конструкт емес [10], нақты мінез-құлықпен қамтамасыз етілген эмпирикалық түрде байқалатын ережелер жиыны.

Бұл процесс моральдық негіздер теориясының [11] тұжырымдарын қайталайды: адами мораль интуитивті, плюралистік және мәдени тұрғыдан өзгермелі. RSN моральдық консенсусты кіріс ретінде талап етпейді; ол мінез-құлықтық консенсусты нәтиже ретінде тудырады. Нәтижесінде пайда болатын қоғамдық келісімшарт статикалық емес—ол қатысушылар қосылған, кеткен және желі кері байланысына жауап ретінде саясаттарын түзеткенде дамиды. Классикалық қоғамдық келісімшарт теориясынан айырмашылығы, бұл келісімшарт қайтарылатын, байқалатын және егемен биліксіз мәжбүрленетін.

8 Экономикалық модель

Алдыңғы бөлімдер құралды—RSN-нің тексеру механизмдерін, шығын құрылымын және эмерджентті консенсусты—сипаттады. Бұл бөлім осы құралды фискалды және басқарушылық көшуге қолдану әдіснамасын сипаттайды. Құрал жалпы мақсатты; төмендегі әдіснама—бір ықтимал қолданыс.

8.1 Ынталандыру құрылымы

Капитал ретіндегі бедел адал мінез-құлық үшін тікелей ынталандыру тудырады. Қалыпты жұмыста қатысушылар күнделікті транзакциялар мен орындалған міндеттемелер арқылы беделді табиғи түрде құрады. Негізгі шығын *теріс* тұжырымдарға жұмсалады—басқалардың келтірген залалын жазуға. Бұл асимметрия

пайдалы, сенімді мінез-құлықты ынталандырады: адал болу қосымша ештеңеге түспейді, ал зиянды болу басқалар сақтауға төлейтін құжатталған із қалдырады. Екіжүзділік—ережелерді ұстанбай мәлімдеу—ең қымбат сәтсіздік режимі, өйткені ол әдейі алдауды көрсетеді.

8.2 Қатарлас фискалды жүйе

Бәсекелестік қысымды үш құрамдас мүмкін етеді: (1) **Қарапайым салық**—ерекшеліксіз бірыңғай пропорционал мөлшерлеме, бастапқыда қолданыстағы нақты мөлшерлемеден шамалы төмен; (2) **Электрондық шығыс тіркеу (Electronic Spending Registration, ESR)**—чех ЕЕТ моделін керісінше айналдырып, азаматтар мемлекеттік шығыстарды бақылайды; (3) **Азамат бағыттайтын салық бөлу**—бірінші жылы бірнеше пайыздан басталып, он жылдан кейін қабылдану қарқынына қарай төмен қос таңбалы санға дейін немесе толықтай азамат бағыттайтын жүйеге дейін жетеді. Нақты қарқын мемлекеттік қызметтерге еркін нарық баламаларының пайда болу жылдамдығына және мемлекеттің көшуге ынтымақтасу ниетіне тәуелді; уақыт функциясы сызықты болуы міндетті емес, ал қабылданудың түпкі жеткен жеріне жоғарғы шек қоюға негіз жоқ.

9 Көшу жолы

Көшу үш кезеңнен өтеді (Fig. 10): **1-фаза: Қаптама** (RSN ақпараттық қабат ретінде, мемлекет жалғыз провайдер), **2-фаза: Бәсекелестік** (RSN функционалды баламалар ұсынады, қос жүйелі қолданыс) және **3-фаза: Көшу** (RSN мемлекеттік баламалардан асып түседі, ерікті көшу). Өту әр кезеңде қайтарылатын.

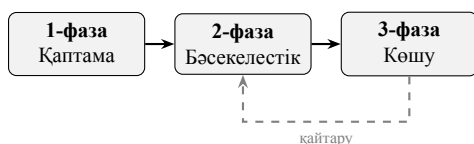


Figure 10: Үш фазалы көшу—әр кезеңде қайтарылатын.

Негізгі қысым механизмі—фискалды: шартты салық төлеушілер «экономикалық маңызды азшылық X »-ке жеткенде—оған қарсы репрессия болмашы емес экономикалық залал келтіретіндей және азаматтық бағынбаушылық сенімді қатерге айналатындай үлкен топ—мемлекет келіссөзге кіріседі. Иллюстрация үшін біз $X \approx 15\%$

ЖІӨ мәнін қолданамыз, бірақ нақты шек нақты экономикаға тәуелді.

10 Қауіпсіздік талдауы

Біз бес қарсылас санатын қарастырамыз: жеке жаман әрекет иелері, ұйымдасқан топтар, корпоративтік қарсыластар, мемлекеттік деңгейдегі қарсыластар және хаттама деңгейіндегі қарсыластар.

Sybil-ге төзімділік [12]. Бедел құру тұрақты, тексерілетін өзара әрекеттестікті талап етеді. Табысты Sybil шабуылының шығыны жалған идентификациялар санына сызықты түрде және нысаналы бедел деңгейіне квадраттық түрде масштабталады. Бірнеше DID-ті қатарлас пайдалану мүмкін, бірақ жоба бойынша қымбат—әр идентификация беделді нақты белсенділік арқылы дербес жинақтауы керек. Еркін қоғамдарда бұл шығын кездейсоқ теріс пайдалануды тежейді; диктатураларда қатарлас DID-тер бөлінген қарсылықты, жасырын үйлестіруді және қара нарықта қауіпсіз бағдарлауды мүмкін ететін өмір сүру құралына айналады.

Астыртын келісімнен қорғаныс. Жабық топтар арасындағы өзара мақұлдау заңдылықтары әлеуметтік граф талдауы арқылы анықталады. Бедел жинақтау функциялары тығыз кластерленген дереккөздердің тұжырымдарын төмендетеді.

Мемлекеттік деңгейдегі қарсылас. Onion бағыттау, орталықтандырылған инфрақұрылымның болмауы және Тексеруші рөлінің қатысушылар арасында таралуы басып тастау кез келген пайдаға сәйкессіз шараларды талап ететінін қамтамасыз етеді.

Құпиялылық пен жауапкершілік. Жалған атпен қатысу—анонимдік пен идентификацияны ашу арасындағы аралық жол—DID-терге иенің нақты дүниедегі тұлғасын ашпай мәнді бедел жинақтауға мүмкіндік береді.

11 Құпиялылық жайттары

RSN-нің құпиялылық моделі жалған атпен қатысуға негізделген. Иесі идентификацияны ашуды бақылайды: ең аз (таза жалған ат), таңдамалы (нақты куәландырулар байланысады) немесе толық (заңды тұлға байланысады). Жарияланған тұжырымдар тұрақты—жүйе контекстілік түзетуді қолдайды, бірақ өшіруді

емес. Иесі бұзылған DID-ті тастап, жинақталған беделден бас тартып, жаңадан баста алады.

12 Байланысты жұмыстар

W3C DID Core спецификациясы [2] және Ceramic Network [8] идентификация негізін қамтамасыз етеді. EigenTrust [13] орталық биліксіз таралған бедел жинақтауды көрсетті. SBT-лер [3] берілмейтін әлеуметтік жетондарды енгізді. RSN экономикалық шығынды сапа сүзгісі ретінде және радикализмді бағалау механизмімен ерекшеленеді.

DAO-лар [4] және квадраттық дауыс беру [5] орталықтандырылмаған басқарудың орындылығын көрсетті. RSN консенсусты дауыс беруден емес, екіжақты баға келіссөздерінен алады.

Ұсыныс жеке қызмет көрсету үшін анархо-капиталистік теорияға [14, 15] сүйенеді, бірақ екі маңызды тұрғыдан ажырайды: ол ұтымдылықты болжаудың орнына кекшілдік пен кек қайтару серпіндеріне жобаланады және революцияның орнына біртіндеп көшуді ұсынады. Эмерджентті қоғамдық келісімшарттар тұжырымдамасының Хайектің стихиялы тәртіп теориясында [16] бастаулары бар.

Анархо-агоризм. RSN агористік қарсы-экономикамен [17] елеулі ортақ негізді бөліседі—әсіресе қатарлас институттар мен ерікті алмасу құруға баса назар аудару жағынан. Алайда агоризм ұтымды өз мүддені жеткілікті үйлестіру механизмі деп болжауға бейім және көбіне қолданыстағы мемлекеттік құрылымдардан нақты көшу жолы жетіспейді. RSN ұтымсыз мінез-құлықтық бейімділіктерді айқын қамтиды және біртіндеп көшу үшін фискалды қысым механизмін ұсынады.

Меритократия. RSN меритократия [18] ұран емес, жүйелік қасиет ретінде қалай пайда бола алатынының алғашқы функционалдық сипаттамасы болуы мүмкін. Дәстүрлі меритократиялық жүйелер сәтсіздікке ұшырайды, өйткені олар «еңбекті» анықтап, оны мәжбүрлеу үшін орталық билікті талап етеді. RSN-де еңбек екіжақты бағалаулардан пайда болады: құндылық жеткізгендер бедел жинақтайды; кімнің еңбегі бар екенін ешбір комитет шешпейді.

Меншік артықшылық ретінде. RSN меншік құқығын табиғи және абсолютті деп қарайтын анархо-капиталистік және австриялық мектеп трактовкаларынан түбегейлі ажырайды. RSN негіздемесінде меншік—*артықшылық*—

қатысушы ортақ нормаларды түбегейлі бұзғанда (сатқындық, экзистенциалдық дағдарыста қауымдастықты қорғаудан бас тарту, жүйелі қанау) шеткі жағдайларда қауымдастық қайтарып ала алатын әлеуметтік тану. Бұл мемлекеттік тәркілеу емес, екіжақты қарым-қатынастар желісінің әлеуметтік тануды қайтарып алуы.

13 Талқылау және шектеулер

Суық бастау. RSN-нің құндылығы желілік әсерлерге тәуелді; ерте қабылдаушылар қатысу шекке жеткенше шектеулі құндылыққа тап болады. Алайда, тіпті ерте кезеңдерден бастап DID желісі пайдалы қосымша ақпарат көзі ретінде қызмет етеді. Ерте бедел бағалауы мен билік бағалауы күрделіліктің артуымен біртіндеп дамиды деп күтіледі.

Leeching-ке қарсы және қолжетімділікті бақылау. Нысана DID-тері беделі төмен DID-тердің сұрауларына кезеңдік алымдар мен қолжетімділік шектеулерін қоя алады. Бұл екілік емес, үздіксіз шкала: сұрау салушы DID-тің беделі неғұрлым аз болса, соғұрлым аз ақпарат алады, соғұрлым ұзақ күтеді және соғұрлым көп төлейді. Бұл механизм енжар тұтынуудан гөрі нақты қатысуды ынталандырады.

Қолжетімділік теңсіздігі. Тұжырымдарды жариялау шығыны экономикалық тұрғыдан қолайсыз қатысушылардың заңды шағымдарын сүзіп тастауы мүмкін. Жеңілдету: әр қатысушы бір мезгілде ықтимал тексеруші ретінде қызмет етеді (немесе бұл рөлді тапсырады) және тексеру алымдарын табады. Жеткілікті уақыт көкжиегінде радикалды емес қатысушы қаржылық бейтараптыққа жақындауы керек—тексеру табысы жариялау шығынын шамамен теңгеруі керек. Бұл—кепілдік емес, статистикалық күтім.

Бедел теңсіздігі. Ерте қабылдаушылар кейін келгендер үшін кедергі тудыруы мүмкін артықшылықтарды жинақтайды. Алайда бедел бағалауын өз жинақтау алгоритмдері арқылы бірінші кезектегі артықшылықты жеңілдетуді таңдай алатын үшінші тарап провайдерлері жүргізеді. Жақсы беделмен бірінші болу—заңды салыстырмалы экономикалық артықшылық—және бұл жоба бойынша солай.

Ашық сұрақтар. Оңтайлы шығын функциялары, жинақтау стандарттары, хаттама басқаруы және ЖИ жасаған синтетикалық бедел деректерімен өзара әрекеттестік болашақ жұмыстың бағыттары болып қала береді.

Бұл мақала RSN барлық жағдайда оңтайлы нәтиже беретінін мәлімдемейді. Ол RSN жүзеге асатын балама екенін мәлімдейді—техникалық тұрғыдан іске асырылатын, экономикалық тұрғыдан өзін-өзі қамтамасыз ететін және адами мінез-құлықтық бейімділіктермен олар шын мәнінде қандай болса, солай әлеуметтік үйлесімді.

14 Қорытынды

Бұл мақала Беделдік әлеуметтік желіні—жалған атпен, тексерілетін бедел алмасуды мүмкін ететін орталықтандырылмаған хаттаманы—ұсынды. Радикализмнің қымбаттылығы қағидаты алаяқтық тұжырымдардың цензурасыз бағамен ысырылып тасталуын қамтамасыз етеді. Ұсынылған көшу жолы қолданыстағы институттардан біртіндеп, қайтарылатын өтуді мүмкін етеді. Жоба адам табиғатын қандай болса, солай—оның ішінде ұсақтық, кекшілдік және кек қайтарудан ләззат алу ынтасын—идеологиялық түрлендіруді талап етудің орнына қамтиды. Нәтиже—утопия емес, әділдік қолжетімді, бедел еңбекпен табылатын және теріс қылық шығынын оны туғызған тарап көтеретін жүйе.

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.