

탈중앙화평판네트워크: 자연스러운사회조직을위한프레임워크

Pavel Kudrna
Prague, Czechia
Draft v1 — March 2026

Abstract

정의감—잘못이바로잡히고공로가보상받는다는확신—은사회를결속시키는가장강력한힘이다. 중앙집권적통치기관이권리를집행하는비용이권리자체의가치를초과하는탓에이감각을제공하지못할때, 사회적결속은침식된다. 현행제도구조는중앙계획이자원배분에실패하는것과체계적으로동일한방식으로상당한부류의분쟁을해결하지못한다. 즉정보비대칭, 피드백루프의부재, 그리고의사결정자가자신의결정이초래하는결과로부터단절되는방식이다. 본논문은평판소셜네트워크 (Reputation Social Network, RSN) 를제시한다. RSN 은탈중앙화식별자 (DID) 를기반으로구축된탈중앙화되고, 부패시킬수없으며, 검열에저항하는통신계층으로서, 가명참여자들이현실세계의행동에관한평판정보를게시하고, 검증하며, 소비할수있게한다. 핵심메커니즘은세가지설계원칙에기반한다. (1) 평판데이터를읽는것은저렴하지만쓰는것은검증가능한노력을요구하는비대칭적비용구조. (2) 일관된해싱 (consistent hashing) 에기반한비결정론적검증자선택프로토콜로, 반복비용의점증을통해급진적주장에가격을매기는방식. (3) 민간검증자가자신이보증하는주장의정확성에자신이축적한평판을거는시장주도형평판권위모델. 그결과로생성되는아키텍처는중앙조정없이실력주의 (meritocracy) 를창발적으로만들어내며, 기존의국가관리체계로부터점진적이고되돌릴수있는이행경로를가능하게한다.

1 서론

1.1 중앙집권적신뢰의문제

현대의통치는근본적인가정에기반한다. 즉중앙집권적기관이낮선사람들사이의신뢰를대규모로중개할수있다는것이다. 법원은분쟁을판결한다. 등기소는소유권을증명한다. 규제기관은표준을집행한다. 이러한기관들은정보가희소하고, 소통이느리며, 중앙기구로의권한위임이유일하게실현가능한조정메커니즘이던시대에설계되었다. 그러나중앙집권적통치는중앙계획과동일한구조적이유로실패한다. 정보비대칭, 피드백루프의부재, 그리고의사결정자가자신의결정이초래하는결과로부터단절되는것이다.

이가정은예컨대제도적중개의비용이분쟁의가치를초

과할때무너진다. 임차한아파트에법적으로요구되는전기안전증명서가없다는것을발견한세입자를생각해보라. 이는생명에즉각적인위험을야기하는상태다. 계약을해지할세입자의법적권리는명백하다. 그러나법원시스템을통해그권리를집행하는비용은, 잠재적인법정배상금을포함하더라도, 보증금과손해배상액의금전적가치를초과한다 [1]. 합리적인대응은손실을감수하고떠나는것이다.

이는병리적인예외사례가아니다. 이는피해는실재하지만금전적이해가제도적집행이경제적으로합리적이되는문턱아래로떨어지는상당한부류의분쟁에서기본적으로겪는경험이다. 그결과논의적행위자에게구조적으로유리한시스템이다. 이문턱아래의규모로타인에게피해를주는자들은처벌받지않고행동할수있는데, 정의를구하는비용이피해를입은당사자에게지워지기때문이다.

위의사례는저자의법적환경—체코의대륙법체계—에서가져온것이다. 다른법전통에서는—판례기반의보통법, 관습법, 혼합체계—관할권의문화적, 절차적특수성에따라정의가서로다른방식과정도로실패한다. 독자들은자신의맥락에서이에상응하는사례를알아볼가능성이크다. 구조적으로보편적인것은그패턴이다. 즉그가치가경제적으로합리적인집행의문턱아래로떨어지는분쟁은피해를입은당사자가손실을떠안는것으로끝난다. RSN 은완벽한정의를약속하지않는다. 다만제도적집행이비경제적일때악의적행위자가누리는구조적이점을줄일뿐이다.

1.2 기존해법이부족한이유

탈중앙화신원 (DID) 프레임워크 [2] 는자기주권적신원관리를위한암호학적메커니즘을제공하지만, 행동평판이라는더넓은문제를다루지않고주로신원검증에초점을맞춘다.

소울바운드토큰 (SBT) [3] 은평판이양도불가능하다는통찰을포착하지만, 확장성제약이있는블록체인인프라에의존하며정보입력을지배하는경제적유인을다루지않는다. 공로토큰 (예: Liberland) 과같은관련개념도유사한철학을공유하지만특정관할권프레임워크에얽매여있다.

탈중앙화자율조직 (DAO) [4] 은스마트계약을통해거버넌스를구현하지만, 영향력이자본에비례하는금권정치적역학을재현한다. 이차투표 (quadratic voting) [5] 는이를부분적으로완화하지만실질적채택을제한한다. DAO 는또한근본적인 오라클문제에직면한다. 스마트계약은신

회할수있는외부출처없이현실세계의상태를안정적으로 검증할수없으며, 이문제는블록체인아키텍처내에서일반적인해법이없다.

기존의어떤시스템도탈중앙화, 검열저항성, 가명성, 검증가능한진입비용, 그리고창발적합의를결합하지못한다.

1.3 기여

본논문은다음과같은기여를한다.

1. DID 프레임워크를확장하여양방향평판교환을지원하는탈중앙화프로토콜인 **평판소셜네트워크 (RSN)** 의정의.
2. 일관된해싱 [6] 에기반한 **비결정론적검증자선택프로토콜**.
3. 세가지복합적비용채널을통해네트워크합의로부터의거리에따라주장에가격을매기는 **급진주의비용화원칙 (Expensive Radicalism Principle)**.
4. 거짓보증이정당한수수료보다파국적으로더큰비용을치르게하는비대칭적유인을지닌 **평판권위 (Reputable Authority) 모델**.
5. 병렬재정인프라를통한 **점진적이행경로**.

2 설계원칙

RSN 아키텍처는다섯가지타협불가능한설계원칙에의해 제약된다.

연속성과진화. 시스템은무기한의이행기간동안기존기관과공존한다. 이행은모든단계에서되돌릴수있어야한다.

자발성과책임. 참여는자발적이지만, 자발성은책임과결합된다. 제도적기능에대한통제권을떠맡는참여자는동시에그에수반되는의무도떠맡는다.

다양성과문화적중립성. 합의는시스템설계자가부과한사전규칙이아니라양방향상호작용에서창발한다.

회복력과검열저항성. 네트워크를검열하는비용은그것을용인하는비용을초과해야한다. 오직완전한전체주의만이—파멸적인정치적, 경제적비용을치르고—시스템을억압할수있다.

합의와집행. 시스템은옹졸함, 양심, 응보적만족을향한인간의경향을하중을지탱하는핵심요소로통합한다. 부정행위는금지되는것이아니라가격이매겨진다.

3 시스템개요

3.1 평판소셜네트워크

RSN 은참여자들이현실세계의행동에관한검증가능한정보를교환하는탈중앙화된 P2P 통신계층이다. 그본질적속성은다음과같다. 탈중앙화되고검열할수없는인프라, DID 를통한가명참여, 비대칭적비용구조 (읽기는저렴하고쓰기는비쌈), 암호학적검증가능성, 그리고 **표준지원**이

다. 표준지원은네트워크를통해전파되는정보, 권위가제공하는서비스 (주장구성, 보증, 증인서비스), 그리고상대방평판을평가하는규칙과 (선언된행동과실제행동간의) 정책불일치위험을평가하는규칙을포함한정책형식에대한기계판독가능한형식을뜻한다.

3.2 아키텍처구성요소

RSN 은네가지주요구성요소로이루어진다 (그림 1).

1. **DID 계층.** 선언된규칙, 평판메타데이터, 네트워크라우팅을갖춘참여자신원.
2. **주장프로토콜 (Claim Protocol).** 현실세계사건에관한단언을게시하기위한구조화된형식.
3. **검증네트워크.** 일관된해싱을사용하여검증자를배정하는탈중앙화프로토콜.
4. **평판집계계층.** 사람이읽을수있는평판요약을생성하는서비스.

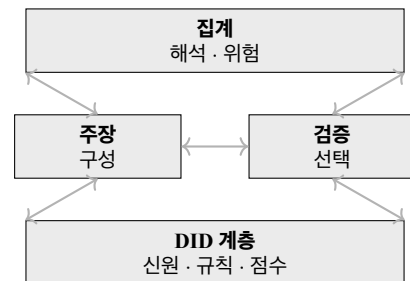


Figure 1: RSN 4 계층아키텍처.

3.3 참여자역할

검증거래에는최대여섯개의구별되는 DID 역할이관여한다 (그림 2). **발행자** (DID_I , 주장을생성하고제출), **대상** (DID_S , 주장이관한 DID—발행자와일치할수있음), **권위** (DID_A , 수수료를받고주장을보증하며증인서비스도제공할수있음—선택사항), **증인** ($DID_{W_{1..n}}$, 챌린지코드를통해검증자의정직성을의명으로감시—선택사항), **검증자** (DID_V , 주장을게시하도록알고리즘으로선택됨), 그리고 **RSN**(검증된주장이게시되는네트워크) 이다. 모든역할은다른 DID 에위임될수있다 (7.4 절). 권위는통상보증과증인서비스를묶어서제공하지만, 두기능은논리적으로독립적이다.

3.4 부패불가능성: 네가지힘

RSN 의부패불가능성은단일메커니즘에서비롯되는것이아니라동시에작용하는네가지힘에서비롯된다. 어느것도그자체로충분하지않다. 오직그것들의결합만이부패시도를경제적으로비합리적으로만든다.

예측불가능한표적. 각주장의검증자는일관된해싱을통해비결정론적으로선택된다 (5.3 절). 검증자의신원은발행자의선택이아니라주장의내용과이전반복의합수이므로, 공격자는매수를위해특정검증자를미리겨냥할수없다.

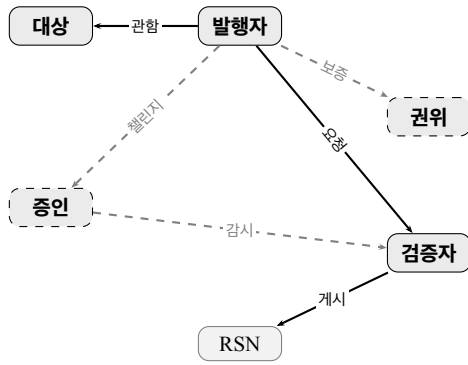


Figure 2: 검증거래에서의 DID 역할. 점선 = 선택사항 (권위, 증인).

평판레버리지—상승은느리고, 하락은빠르다. 평판은 지속적인 일관된 행동을 통해 점진적으로만 얻을 수 있다. 그러나 단 한번의 사기성 보증으로 파국적으로 잃을 수 있다 (6.2 절). 이비대칭은 수년간 축적한 평판이 단 한번의 부정직한 보증으로 파괴될 수 있음을 뜻한다. 최적의 전략은 여전히 의심스러운 주장을 거부하는 것이다.

공개적 약속. 모든 DID 보유자는 자신의 정책—따르기 로 약속한 기계판독 가능한 규칙의 집합—을 공개적으로 선언한다. 선언과 실제 행동 사이의 괴리는 탐지 가능하며 근본적인 위반보다 더 심각한 평판 위반으로 가격이 매겨진다 (7.3 절). 따라서 위선은 직접적인 부정직함보다 더 큰 비용을 치른다.

메시 (mesh) 공격비용 비대칭. 네트워크를 검열하거나 불안정하게 만드는 비용은 네트워크의 규모와 밀도에 따라 비선형적으로 증가하는 반면, 그것을 용인하는 비용은 일정하게 유지된다. 검열이 수지를 맞추려면 중앙집권적 행위자가 그것을 네트워크 전체에 적용해야 하는데, 이는 어떤 상상 가능한 이익과도 비례하지 않는 조치를 요구한다 (10 절).

4 탈중앙화 신원 모델

4.1 특수 속성을 지닌 DID

RSN은 W3C DID Core 명세 [2]를 다음으로 확장한다. **선언된 규칙** (기계판독 가능한 행동 약속), **평판 메타데이터** (집계된 행동 점수), 그리고 **네트워크 라우팅** (안정적인 링 위치와 분리된 가변적 어니언 게이트웨이).

4.2 주장 생애주기

주장은 여섯 단계를 거친다 (그림 3). 구성, 선택적 권위 보증, 일관된 해시를 통한 검증자 선택, 검증 결정 (수락 또는 반복 포함 거부), 게시, 그리고 모든 당사자에 대한 평판 갱신이다.

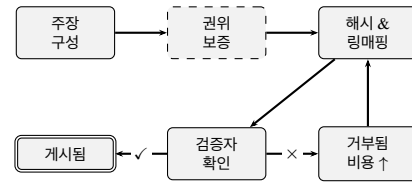


Figure 3: 반복 루프를 지닌 주장 생애주기.

4.3 W3C DID Core와의 관계

RSN의 신원 모델은 W3C DID Core 명세 [2]의 진부분 집합의 상위 집합이다. 모든 RSN DID는 유효한 W3C DID다. RSN 고유의 확장은 전용 DID 방식 명세에 정의된 DID 문서 속성으로 인코딩되며, ION [7]과 Ceramic [8] 같은 기존 인프라와 호환된다.

5 정보 검증과 전파

5.1 정보 진입 비용

RSN의 핵심 경제 원칙은 읽기와 쓰기 사이의 비대칭이다. 평판 데이터를 읽는 것은 DID 네트워크의 일부이고 자신의 평판에 상응하는 접근 권한을 가진 참여자에게 한계 비용이 0에 가깝다—신규 참여자는 점진적으로 더 넓은 접근 권한을 얻어야 한다 (반 (反) 무임승차 참조). 쓰기—일회성 기술적 행위거나 아니라 평판을 네트워크에 지속적으로 구현하는 것으로 이해되는—는 세차원에 걸친 검증 가능한 누적 투자를 요구한다. **시간** (일관된 행동, 이행된 약속, 가꾼 관계에 쓰인 인생의 세월), **에너지** (정직한 거래, 협력 관계에 대한 배려, 장기적 신뢰성에 투자한 노력), 그리고 **돈** (자신의 이름에 대한 투자—전문성 개발, 자기 일의 품질, 초래한 피해에 대한 배상)이다. 평판은 즉시 살 수 없다—그것은 시스템이 그저 가시화하고 맥락을 넘어 이전 가능하게 만들 뿐인, 평생에 걸친 축적의 결과다. 프로토콜의 일회성 기술 비용 (암호학적 서명, 검증자 수수료)은 이 근본적 투자에 비하면 무시할 만하다.

5.2 소셜 그래프와 접촉 깊이

RSN은 근본적으로 소셜 네트워크다. 각 DID는 연결을 허용하는 접촉자 (다른 DID)를 추가한다. 이 접촉자들은 자신의 접촉자를 가지며, 그런 식으로 이어진다. 알고리즘적 검증자 탐색은 연결된 접촉자의 설정 가능한 깊이 h 이내에 시작된다 (예: $h = 3$: 자신의 직접 접촉자, 그들의 접촉자, 그리고 접촉자의 접촉자). 이야기 텍처는 단일 글로벌 록체인을 요구하지 않는다—그것은 자연스럽게 다른 커뮤니티와 겹치는 커뮤니티/클러스터의 창발을 선호한다. 모든 DID 참여자는 게시된 **정책**—들어오는 요청을 어떻게 평가할지 지배하는 기계판독 가능한 규칙의 집합—을 가져야 한다. 정책 위반은 부정적 아티팩트로 네트워크에 기록된다.

5.3 알고리즘적검증자선택

검증프로토콜은일관된해싱 [6] 을사용한다 (그림 4). 검증은유료서비스다. 검증자는수수료를받고운영하며, 이는경쟁이가격, 속도, 신뢰성을건인하는시장을만든다.

1 단계. 주장문서는이전반복의해시결과 (또는첫반복에서는 $\emptyset$) 와연결되어해싱된다.

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

알고리즘은단지이전반복의해시가아니라모든이전요청과응답의 완전한경로를포함해야한다. 각검증자의전체응답 (수락, 거부, 제시된가격, 사유) 은커져가는문서에추가되며, 각단계에서암호학적서명을통해검증가능하다.

2 단계. 해시는일관된해시링위의 N 개위치에매핑되며, 이는균등하게분포된다 (예: $N = 4$ 의경우 $+0^\circ, +90^\circ, +180^\circ, +270^\circ$). 각위치에서시계방향탐색이가장가까운 DID 를검증자후보로선택한다 (그림 5). N 은현재활성 DID 의비율, 하루중시각, 또는과거네트워크응답성에따라달라질수있는가변매개변수다.

3 단계. 검증자는 (평판을걸고게시하며) 수락하거나, (거부해시와함께 1 단계로돌아가) 거부한다. 온라인상태를선언했음에도노드가응답하지않을때, 다음요청은이전 N 개검증자후보모두의응답을포함해야한다.

반 (反) 무임승차. 대상 DID 는평판이적은신규 DID 의조회에대해수수로나접근제한을설정할수있다. 이점진적메커니즘 (이분법이아님) 은신규참여자타인의데이터를자유롭게소비하기전에진정한활동을통해평판을쌓도록강제한다.

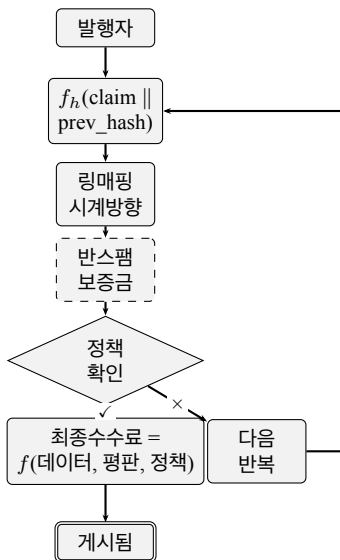


Figure 4: 검증자선택프로토콜. 반스팸보증금은선택사항이며한불가능할수있다. 최종수수료는수락시에만지불된다.

각거부는검증자의전체응답 (사유와조건포함) 을주장문서에추가하여그내용을확장한다. 확장된문서로부터새로운해시가비결정론적으로계산되어다른링위치에매핑되고다른검증자를선택한다. 전체경로의문서화는필수

다—발행자는다음검증자를예측하거나영향을미칠수없다. 검증자가호환되는선언정책에도불구하고요청을무시하면, (증인이있는경우) 증인이이를기록하고, 발행자는최종게시시증인증거를첨부할수있다.

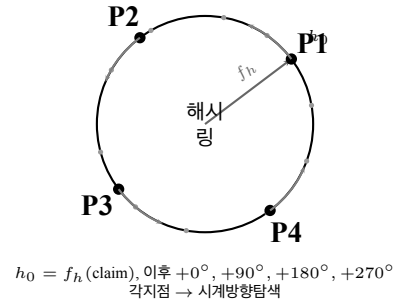


Figure 5: 다중지점선택 ($N=4$). 해시 h_0 가오프셋을설정하고, h_0 에서균등하게분포된 4 개지점.

5.4 증인프로토콜

증인역할은암호학적챌린지코드프로토콜을통해검증자의정직성에대한의명의책임성을제공한다.

W1 단계. 요청자는검증요청에서명하고이를 N_w 명의증인—요청자의소셜네트워크의접촉자, 또는수수료를받고운영하는전문증인서비스제공자—에게보낸다.

W2 단계. 각증인 w_i 는서명된전체요청에서명하고, 원본서명 σ_i 를보관하며, 챌린지코드 $c_i = h(\sigma_i)$ 를계산한다. 챌린지코드는요청에추가된다.

W3 단계. 이제 N_w 개의챌린지코드를지닌요청이검증자에게전송된다. 검증자는코드를관찰하지만누가증인인지, 또는코드가실제서명에대응하는지 판별할수없다.

W4 단계 (정직한검증자). 검증자가선언된정책에따라응답하면, 챌린지코드는불투명하게남는다. 증인은결코드러나지않는다. 추가데이터는게시되지않는다.

W5 단계 (정책위반). 검증자가정책을위반하면 (요청 무시, 일관되지않은응답), 요청자는증인의원본서명 σ_i 를보유하고있다. 이는동반데이터로게시될수있다. 누구든 $c_i = h(\sigma_i)$ 를검증하여증인이있었음을증명할수있다. 검증자는이미응답에서챌린지코드에서명했으므로요청자는독립적으로게시할수있다.

블러프 (bluff) 속성. 요청자는일부또는모든챌린지코드를무작위값으로대체할수있다. 검증자는진짜코드 (고평판권위가뒷받침하는) 를잡음과구별할수없다. 이 불확실성이집행메커니즘이다. 모든요청은준경보는권위가의명인지커보고있을위험을수반한다. 이압박을유지하는비용은 0 에가깝지만 (무작위숫자생성), 검증자에게부정직함이초래할잠재적비용은파국적이다. 실제증인이없더라도정직한행동이장려된다.

증인으로서의권위. 주장을보증하는권위는증인서비스를뭉을수있다. “나는당신의주장을보증하며검증동안의명의증인으로활동한다.” 이는자연스러운사업모델이다—권위는이미맥락을가지고있다. 그러나두역할은논리

적으로 독립적이다.

5.5 급진주의비용화원칙

세가지비용채널이동시에복합된다 (그림 6).

채널 1: 반복비용. 각거부는시간과자원을소비하는새로운반복을강제한다. 선형증가.

채널 2: 문서팽창. 각반복은검증자의전체응답을주장문서에추가한다. 증가는선형이지만기저오프셋이있다. 초기페이로드 (주장내용, 권위보증, 암호학적서명) 는이미무시할수없는크기 B_0 를가진다. k 번반복후전체크기는 $S(k) = B_0 + k \cdot \Delta$ 이며, 여기서 Δ 는평균응답크기다.

채널 3: 검증자위험프리미엄. 위험은주관적이다. 검증자는요청하는 DID 의선언된정책이검증자자신의상업적, 사회적, 또는정치적이해와충돌하는지평가한다. 프리미엄은검증자의 “이상” 으로부터의인지된거리에따라지수적으로상승할수있다. $P(d) = \alpha \cdot e^{\beta d}$, 여기서 d 는검증자의주관적거리척도다. 개인적금지선 (no-go boundary) 을넘어서면검증자는전면적으로거부할수있다.

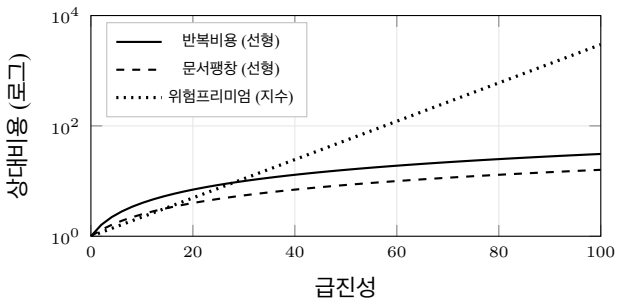


Figure 6: 세채널에걸친비용상승. 위험프리미엄이높은 급진성에서지배적이다.

결정적으로, 이것은검열이아니다. 어떤주장도금지되지않는다. 시스템은위험에가격을매긴다 (표 1).

Table 1: 주장유형별비용비교.

유형	반복	문서	수수료	총계
신뢰성있음	$k_{\min}$	B_0	$P_{\min}$	낮음
논쟁적	k_{med}	$B_0 + k\Delta$	$\alpha e^{\beta d}$	중간
급진적	$k_{\max}$	$\gg B_0$	$\gg P_{\min}$	매우높음
사기성	$\rightarrow \infty$	—	—	계시불가

6 평판과위험평가

6.1 평판축적모델

평판은세가지속성을보인다. **느린축적** (일관된행동을 통한점진적성장), **빠른파괴** (단한번의사기가점수를파국적으로떨어뜨릴수있음), 그리고 **개별적평가** (각소비당사자가자신만의집계함수를적용할수있음) 다.

6.2 평판권위

평판권위는주장을검토하고, 만족하면이를공동서명한다—자신의평판을건다 (그림 7). 비대칭은의도된설계다. 평판을얻는것은느리지만 (정직한보증마다점진적 $+\delta$), 잃는것은파국적이다 (거짓보증마다 $-\Delta \gg \delta$; 예시로 $+2\%$ 대 -70%). 최적의전략은언제나의심스러운주장을거부하는것이다. δ 와 Δ 의구체적값은시스템매개변수다.

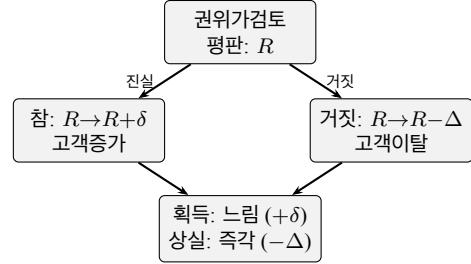


Figure 7: 평판권위—비대칭적유인.

6.3 다차원평판

평판은스칼라가아니라여러차원에걸친벡터다. 재정적신뢰성, 개인적성실성, 전문적역량, 시민적참여등 (그림 8). 서로다른평가제공자는맥락에따라이벡터를다르게투영한다—대출기관은재정적신뢰성을, 고용주는전문적역량을, 이웃은시민적행동을우선시한다. 단하나의 “올바른” 평판점수는없다. 오직관점만이있을뿐이다.

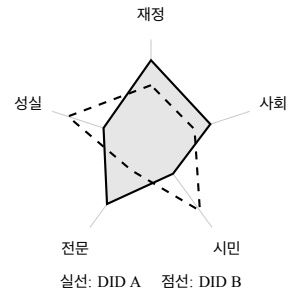


Figure 8: 다차원평판벡터. 서로다른 DID 는차원에걸쳐서로다른프로필을보인다.

6.4 위험평가의민주화

RSN 은체계적위험평가를민주화한다—현재금융기관에 집중되어있지만은행업을훨씬넘어적용가능한역량이다. 공급자신뢰성을평가하는산업대기업, 행동위험에가격을매기는보험사, 인수합병을위한실사, 제조업에서의장비수명추정—상대방위험평가가필요한곳이면어디서든 RSN 은탈중앙화되고시장주도적인대안을제공한다. 해석서비스시장은원시다차원평판데이터를실행가능한요약으로번역하여, 어떤참여자든한계비용으로상대방평가에접근할수있게한다.

7 합의와분쟁해결

7.1 탈중양화정의모델

RSN 은정의양방향협상문제로재구성한다. 영구적이고검증가능한평판훼손의위험은피해를입은당사자가감당할수없는법적절차보다더효과적인억지력이다.

7.2 창발적합의

각참여자개인의만족문턱을유지한다. 네트워크의집합적합의는수천건의양방향협상의통계적평균으로창발한다(그림 9). 합의를크게상회하는대응(야만적)은게시하기에비싸다. 합의에근접한대응(비례적)은저렴하다. 합의는규칙이아니다—그것은가격신호다.

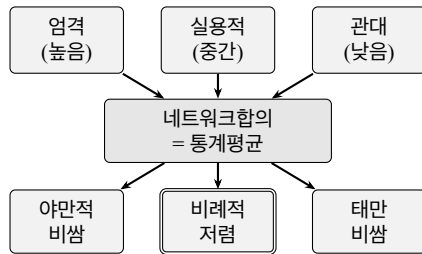


Figure 9: 개인적만족문턱으로부터의창발적합의.

7.3 처벌보정

각 DID 보유자는특정부정행위범주에대한대응을공개적으로선언한다. 불균형하게가혹하거나관대한선언은부정적평판신호를끌어들인다. 비례적선언은마찰없이수용된다—자기보정적처벌시스템이다.

합의선언자체도위선타미지대상이다. 합의입장에선언적으로약속하면서일관되지않게행동하는것은의도적기만을드러내므로, 근본적일탈보다더심각한평판위반을구성한다.

7.4 위임

DID 내의모든활동은—한가지예외를제외하고—다른 DID 에위임될수있다. **대상역할—주장이그행동에관한 DID—은위임될수없다. 그것은주장이지칭하는신원보유자에게양도불가능하게결속된다.** 다른능동적역할—발행자, 권위, 증인, 검증자—은검증, 주장제출, 합의참여, 또는분쟁해결을위해지정된대리 DID 에이전될수있다. 위임은언제든철회가능하다. 이는보유자가궁극적통제권과책임을유지하면서전문화(예: 전문검증서비스)를가능하게한다. 위임은시스템전반에적용되며확장성에필수적이다.

7.5 개인의도덕에서창발적사회계약으로

각 DID 의선언된정책은개인의도덕의형식화를나타낸다. 즉보유자가무엇을수용가능하다고여기는지, 특정행동에어떻게대응하는지, 상대방에게무엇을요구하는지다. 이 정책들은시스템설계자가부과하는것이아니다—각참여자자가선택하고기계판독가능한형식으로표현한다.

이형식화는세단계의창발을가능하게한다. 첫째, 개인도덕은 **정책**—DID 가따르기로약속한선언된규칙, 문턱, 대응함수의집합—으로인코딩된다. 둘째, 네트워크전반의모든정책의집합은 **창발적윤리**—어떤단일참여자도설계하지않았지만수천개의개별도덕적입장의상호작용에서발생하는, 통계적으로관찰가능한규범 [9]—를산출한다. 셋째, 양방향가격신호를통해집행되는공유된행동규범으로표현된이창발적윤리는 **측정가능한사회계약**을구성한다—아무도서명하지않은이론적구성물 [10] 이아니라, 실제행동으로뒷받침되는경험적으로관찰가능한규칙의집합이다.

이과정은도덕기반이론 [11] 의발견을반영한다. 인간의도덕은직관적이고, 다원적이며, 문화적으로가변적이다. RSN 은입력으로도덕적합의를요구하지않는다. 그것은출력으로행동적합의를산출한다. 그결과로나온사회계약은정적이지않다—참여자가가입하고, 탈퇴하고, 네트워크피드백에반응하여정책을조정함에따라진화한다. 고전적사회계약이론과달리, 이계약은철회가능하고, 관찰 가능하며, 주권자없이도집행가능하다.

8 경제모델

앞선절들은도구—RSN 의검증메커니즘, 비용구조, 창발적합의—를설명했다. 이절은이도구를재정및거버넌스이행에적용하는방법론을설명한다. 도구는범용적이며, 아래의방법론은하나의가능한응용이다.

8.1 유인구조

자본으로서의평판은정직한행동에대한직접적유인을만든다. 정상적인운영에서참여자는일상적거래와이행된약속을통해자연스럽게평판을쌓는다. 주된지출은 부정적주장—타인이저지른피해를기록하는것—에쓰인다. 이비대칭은유용하고신뢰할수있는행동을장려한다. 정직한것은추가비용이들지않는반면, 해로운것은타인이보존하는데기꺼이비용을치를문서화된흔적을만든다. 위선—규칙을선언하고따르지않는것—은가장비싼실패양태다. 그것이의도적기만을드러내기때문이다.

8.2 병렬재정시스템

세가지구성요소가경쟁압력을가능하게한다. (1) **단순세**—예외없는단일비례세율로, 초기에는기존실효세율보다근소하게낮게. (2) **전자지출등록 (ESR)**—체코의 EET 모델을뒤집어서민이국가지출을감시하도록함. (3) **시민**

지정세금배분—첫해에몇퍼센트로시작하여 10 년후에는 채택속도에따라낮은두자릿수부터시민지정시스템으로의 완전한이행에이르기까지. 실제속도는국가서비스에대한 자유시장대안이나타나는속도와이행에협력하려는국가의 의지에달려있다. 시간의함수는선형일필요가없으며, 채택이궁극적으로도달할지점에상한을설정할이유는없다.

9 이행경로

이행은세단계를거쳐진행된다 (그림 10). **1 단계: 오버레이** (RSN 이정보계층으로작동, 국가가유일한제공자), **2 단계: 경쟁** (RSN 이기능적대안제공, 이중시스템사용), 그리고 **3 단계: 이행** (RSN 이국가등가물물능가, 자발적 이주). 이행은모든단계에서되돌릴수있다.

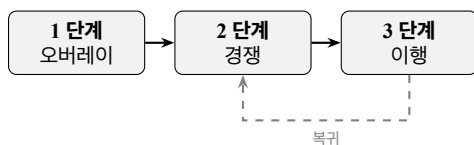


Figure 10: 3 단계이행—모든단계에서되돌릴수있음.

주된압력메커니즘은재정적이다. 조건부납세자가 “경제적으로유익미한소수 X ”—그에대한억압이무시할수없는경제적피해를초래하고시민불복종이신빙성있는위협이 될만큼충분히큰집단—에도달하면, 국가는협상에들어간다. 예시를위해 $X \approx \text{GDP}$ 의 15% 를사용하지만, 실제 문턱은특정경제에달려있다.

10 보안분석

우리는다섯가지적대자범주를고려한다. 개인악의적행위자, 조직된집단, 기업적대자, 국가수준적대자, 그리고프로토콜수준적대자다.

시빌 (Sybil) 저항 [12]. 평판을쌓는것은지속적이고검증가능한상호작용을요구한다. 성공적인시빌공격의비용은가짜신원의수에따라선형적으로, 목표평판수준에따라이차적으로증가한다. 여러 DID 를병렬로운영하는것은가능하지만설계상비싸다—각신원은진정한활동을통해 독립적으로평판을축적해야한다. 자유사회에서이비용은안일한남용을억제한다. 독재국가에서병렬 DID 는구획화된저항, 지하조정, 더안전한암시장항해를가능하게하는생존도구가된다.

공모방어. 폐쇄된집단내의상호보증패턴은소셜그래프 분석을통해탐지가능하다. 평판집계함수는긴밀하게군집된출처의주장을할인한다.

국가수준적대자. 어머니라우팅, 중앙집권적인프라의 부재, 그리고참여자기반전반에걸친검증자역할의분산은억압이어떤이익과도비례하지않는조치를요구하도록보장한다.

프라이버시대책임성. 가명성—익명성과신원공개사이

의중간지대—은 DID 가보유자의현실세계신원을드러내지않고도의미있는평판을축적할수있게한다.

11 프라이버시고려사항

RSN 의프라이버시모델은가명성에기반한다. 보유자는신원공개를통제한다. 최소 (순수가명), 선택적 (특정자격 증명연결), 또는완전 (법적신원연결) 이다. 게시된주장은영구적이다—시스템은맥락적정정은지원하지만삭제는지원하지않는다. 보유자는손상된 DID 를버리고축적한평판을포기하며새로시작할수있다.

12 관련연구

W3C DID Core 명세 [2] 와 Ceramic Network [8] 는신원기반을제공한다. EigenTrust [13] 는중앙권위없는분산평판집계를입증했다. SBT [3] 는양도불가능한사회적토큰을도입했다. RSN 은품질필터로서의경제적비용에 대한강조와급진주의에가격을매기는메커니즘에서차별화된다.

DAO [4] 와이차투표 [5] 는탈중앙화거버넌스의실현가능성을입증했다. RSN 은투표가아니라양방향가격협상으로부터합의를도출한다.

이제안은민간서비스제공에관해무정부자본주의이론 [14, 15] 에기대지만두가지결정적측면에서벗어난다. 즉합리성을가정하기보다양심과응보적충동을위해설계하며, 혁명이아니라점진적이행을제안한다. 창발적사회계약이라는개념은하이에크의자생적질서 (spontaneous order) 이론 [16] 에선례를둔다.

무정부아고리즘 (anarcho-agorism). RSN 은아고리스트대항경제학 [17] 과상당한공통기반을공유한다—특히병렬제도구축과자발적교환에대한강조에서다. 그러나아고리즘은합리적자기이익을충분한조정메커니즘으로가정하는경향이있으며, 기존국가구조로부터의구체적이행경로가결여된경우가많다. RSN 은비합리적행동경향을 명시적으로통합하고점진적이행을위한재정적압력메커니즘을제공한다.

실력주의 (meritocracy). RSN 은실력주의 [18] 가구호가아니라시스템적속성으로어떻게창발할수있는지에대한최초의기능적서술을나타낼수있다. 전통적실력주의시스템은 “실력” 을정의하고집행할중앙권위를요구하기때문에실패한다. RSN 에서실력은양방향평가로부터창발한다. 가치를제공하는자는평판을축적하며, 어떤위원회도누가실력을가졌는지결정하지않는다.

특권으로서의재산. RSN 은재산권을자연적이고절대적인것으로다루는무정부자본주의및오스트리아학파의취급에서근본적으로벗어난다. RSN 프레임워크에서재산은 특권—극단적인경우참여자가공유된규범을근본적으로위반할때 (배신, 실존적위기에서공동체를방어하기를거부, 체계적착취) 공동체가철회할수있는사회적인

정—이다. 이것은 국가의 물수가 아니라 양방향 관계 네트워크에 의한 사회적인 정의 철학이다.

13 논의와 한계

콜드스타트. RSN 의가치는 네트워크 효과에 달려 있다. 초기 채택자는 참여가 문턱에도 달할 때까지 제한된 가치에 직면한다. 그러나 초기 단계부터 DID 네트워크는 유용한 보조 정보원으로 기능한다. 초기 평판 평가와 권위 평가는 정보 함이 증가하며 점진적으로 발전할 것으로 예상된다.

반 (反) 무임승차와 접근 제어. 대상 DID 는 저 평판 DID 의 조회에 점진적 수수료와 접근 제한을 부과할 수 있다. 이는 이분법이 아니라 연속적 척도다. 조회하는 DID 가 평판이 적을수록 받는 정보가 적고, 더 오래 기다리며, 더 많이지불한다. 이메일 키즈는 수동적 소비보다 진정한 참여를 장려한다.

접근의 불평등. 주장을 게시하는 비용은 경제적으로 불리한 참여자의 정당한 불만을 걸러낼 수 있다. 완화책: 모든 참여자는 동시에 잠재적 검증자로 기능하며 (또는 이 역할을 위임하며) 검증 수수료를 본다. 충분한 시간 지연에 걸쳐, 급진적이지 않은 참여자는 재정적 중립—검증 소득이 게시 비용을 대략 상쇄하는—에 접근해야 한다. 이는 통계적 기대이지 보장이 아니다.

평판 불평등. 초기 채택자는 후발 주자에게 장벽이 될 수 있는 이점을 축적한다. 그러나 평판 평가는 제 3 자 제공자가 수행하며, 이들은 자신의 집계 알고리즘을 통해 선점 이점을 완화하는 쪽을 선택할 수 있다. 좋은 평판으로 먼저 있는 것은 정당한 비교 경제적 이점이며—그것은 의도된 설계다.

미해결 질문. 최적 비용 함수, 집계 표준, 프로토콜 거버넌스, 그리고 AI 생성 합성 평판 데이터와의 상호 작용은 향후 연구 영역으로 남는다.

본 논문은 RSN 이 모든 상황에서 최적의 결과를 산출할 것이라고 주장하지 않는다. 본 논문은 RSN 이 실현 가능한 대안—기술적으로 구현 가능하고, 경제적으로 자기 지속적이며, 있는 그대로의 인간 행동 경향과 사회적으로 양립 가능한—을 나타낸다고 주장한다.

14 결론

본 논문은 가명적이고 검증 가능한 평판 교환을 가능하게 하는 탈중앙화 프로토콜인 평판 소셜 네트워크를 제시했다. 급진 주의 비용화 원칙은 사기성 주장이 검열 없이 가격에서 배제되도록 보장한다. 제안된 이행 경로는 기존 기관으로부터의 점진적이고 되돌릴 수 있는 이행을 가능하게 한다. 이 설계는 이념적 변혁을 요구하기보다—용졸함, 양심, 응보적 만족에 대한 욕구를 포함하여—있는 그대로의 인간 본성을 통합한다. 그 결과는 유토피아가 아니라 정의에 접근할 수 있고, 평판이 획득되며, 부정행위의 비용이 그것을 초래한 당사자에 의해 부담되는 시스템이다.

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. Ohlhaber, 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.