The Reputation Circulation Standard (RCS): A Post-Scarcity Economic Protocol V1.0

Arifa Khan

1 August 2025

Abstract

When machines produce everything, only contribution remains scarce.

Artificial intelligence collapses the marginal cost of production, rendering price signals ineffective. Markets, optimized for scarcity, fail to coordinate when labor is infinite and goods cost nothing. Traditional economic primitives—capital, ownership, and exchange—cease to function.

We present the Reputation Circulation Standard (RCS): a computable protocol for post-scarcity coordination. Agents earn Individual-Bound Reputation Units (RUs) through verifiable public contribution. Each RU decays exponentially:

$$R(t) = R_0 \cdot e^{-\lambda t}$$

This single function transforms reputation from static legacy into dynamic *proof-of-relevance*. No influence persists without renewal. Reputation becomes non-transferable, perishable, and mathematically bounded.

RCS establishes reputation as an economic primitive. The protocol implements:

- Dual-token architecture separating governance (RU) from utility (RCS);
- Domain-specific decay rates calibrated to knowledge velocity;
- Multi-layer verification through zero-knowledge proofs and AI-human adjudication;
- Logarithmic wealth adjustment preventing plutocratic capture;
- Commons amplification ($\alpha > 1$) reversing public goods underproduction;
- Integration with identity verification systems for Sybil resistance;
- Universal Basic Reputation (UBR) ensuring minimum participation for all participants.

We prove convergence to equilibrium at $R^* = \mu/\lambda$, where issuance equals decay. The system admits human and artificial agents symmetrically, preserving agency even as intelligence becomes commodified. At Nash equilibrium, continuous contribution dominates all other strategies.

RCS solves the tragedy of the commons through perishable trust.

In the post-scarcity economy, where labor is infinite and intelligence abundant, reputation becomes money, because it decays like memory.

1. A World Without Prices

What happens when the cost of anything becomes nothing?

As artificial intelligence drives marginal cost toward zero, price collapses as a signal. Labor, goods, and services become abundant. But coordination does not.

The old pillars—scarcity, price, and capital—no longer align human effort with collective good.

Markets fail where value cannot be priced:

- Public goods go unrewarded.
- Wealth concentrates without contribution.
- Incentives drift from relevance to rent.

Civilization requires a new substrate—one that can signal trust, alignment, and contribution in a world where supply is infinite.

2. Contribution as Coordination

In the absence of prices, contribution becomes coordination.

The Reputation Circulation Standard (RCS) introduces a formal system for measuring it:

- **Reputation Units (RUs):** individual-bound tokens earned through verified acts.
- **Exponential Decay:** RUs fade unless renewed.
- **Wealth Adjustment:** Influence scales logarithmically with wealth.
- **Commons Amplification:** Public goods receive higher weight.

Each RU is cryptographically issued, time-sensitive, and domain-specific. Together, they form a contributor's Unified Reputation Index (URI)—a living ledger of societal alignment.

Both human and AI agents earn RUs through contributions, with identity persistence handled through cryptographic keys rather than biometric anchors.

Reputation decays like memory. Trust must be renewed.

3. The Core Insight

Where Bitcoin used computation to prove work, RCS uses time to prove relevance.

$$R(t) = R_0 \cdot e^{-\lambda t}$$

This equation turns reputation from legacy into signal—enforcing renewal, eliminating stasis, and dissolving inherited authority.

Only contributors govern. Only contributors remain.

4. Design Principle

You are what you have contributed—recently.

RCS makes this rule computable. Its architecture is:

- Mathematically governed
- Cryptographically verifiable
- Immune to hoarding

Where price fails, **reputation flows**—tracking relevance, rewarding renewal, and amplifying public good.

No legacy can be inherited. No influence is permanent.
Reputation becomes a living currency of trust.

5. Civilization Blueprint

Beyond scarcity lies a new architecture of human coordination.

RCS offers a concrete architecture for abundance where contribution, not capital, governs influence and coordination.

6. System Design

6.1 Formal Reputation Function

Complete System Summary

Reputation Sources:

- Universal Basic Reputation (UBR)
- Earned through contributions
- Earned through donations (wealth-adjusted)

Key Properties:

- Exponential decay over time
- Domain-specific parameters
- Non-transferable
- Wealth-adjusted for fairness

Unified Reputation Index

The Unified Reputation Index equals the total reputation across all domains:

$$URI = UBR + RU_{donation} + \sum_i \left[RU_{earned}(i) \times e^{-\lambda_i \times t} \right] \tag{1}$$

where: UBR = Universal Basic Reputation, λ_i = domain-specific decay rate, t = time

Core Reputation Formulation

Total reputation equals base reputation plus donation-derived reputation:

$$\mathrm{RU}_{\mathrm{total}}(t) = \mathrm{RU}_{\mathrm{base}}(t) + \mathrm{RU}_{\mathrm{donation}}(t) \tag{2}$$

Base reputation includes UBR plus all earned RUs with domain-specific decay:

$$\mathrm{RU}_{\mathrm{base}}(t) = \mathrm{UBR} + \sum_i \left[\mathrm{RU}_{\mathrm{earned}}(i, 0) \times e^{-\lambda_i \times t} \right] \tag{3}$$

Earned Reputation

$$\mathrm{RU}_{\mathrm{earned}}(i) = \alpha_i \times C_i \times V_i \tag{4}$$

- α_i = Commons multiplier (domain i)
- C_i = Contribution impact
- V_i = Verification confidence [0,1]

where $V_i = \frac{\text{verifier agreements}}{\text{total verifiers}} \times$ verifier reputation weight

Donation Reputation

$$\mathrm{RU}_{\mathrm{donation}} = \beta \times D \times g(W_i) \tag{5}$$

where β = [50, 200] RU per (\$)1000 donated, calibrated per deployment

- β = Donation coefficient
- D = Donation amount (\$)
- $g(W_i)$ = Wealth adjustment function

Key Functions

Universal Basic Reputation

$$\mathrm{UBR} = \gamma \times \text{participation\_status} \tag{6}$$

where γ = base amount (e.g., 100 RU)

Wealth Adjustment

$$g(W_i) = \begin{cases} 1 & \text{if } W_i \leq W_{\mathrm{threshold}} \\ \dfrac{\log(1 + W_{\mathrm{threshold}})}{\log(1 + W_i)} & \text{if } W_i > W_{\mathrm{threshold}} \end{cases} \tag{7}$$

Voting Power

$$V(i) = \sqrt{\mathrm{RU}_{\mathrm{total}}(i)} \tag{8}$$

Quadratic voting mechanism

6.2 Economic Primitives

Reputation Unit (RU): Individual-bound token representing verified contribution. These units form the atomic element of the reputation economy, non-transferable and time-sensitive by design.

Unified Reputation Index (URI): aggregating cross-domain reputation. This index provides a holistic measure of an individual's contribution across multiple fields of endeavour. URI is linearly additive since it is domain weighted, and comparable to another individual's URI.

6.3 Contribution Valuation

For direct contributions:

$$\mathrm{RU}_{\mathrm{earned}}(i) = \alpha_i \times \mathrm{Impact}_i \times \mathrm{Verification}_i \tag{9}$$

Where α_i is the commons multiplier for domain i

Impact_i = Log-scale reach/significance

$\mathrm{Verification}_i$ = Confidence score [0,1]

6.4 Wealth Adjustment

To prevent plutocratic capture while enabling meaningful contribution from wealth, we propose a wealth adjustment to RU (donation), reputation earned by donating money (not RU) to UBI pools.

$$\mathrm{RU}_{\mathrm{donation}} = \beta \times D \times \frac{\log(1 + W_{\mathrm{threshold}})}{\log(1 + W_i)} \tag{10}$$

Where:

- D = Donation amount (real money not RU)
- W_i = Individual wealth

Logarithmic formulation ensures wealthy individuals can contribute meaningfully while preventing the direct purchase of influence. Incentives align to eliminate the need to contribute to n different charities. See Appendix D.3 for suggestions on $W_{\mathrm{threshold}}$.

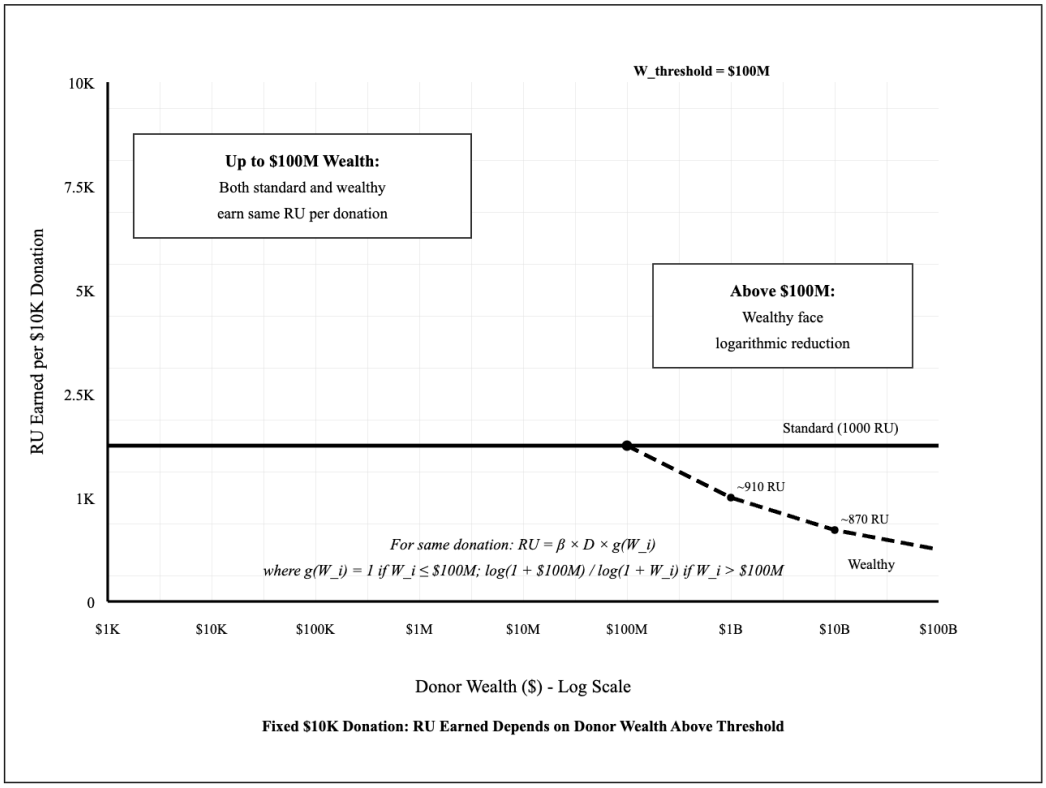

Figure 1: WEALTH-ADJUSTED RU EARNING CURVES

7. Core Mechanism

7.1 Core RU Properties

Reputation Units possess four fundamental properties:

- **Non-transferable:** Preventing markets and speculation
- **Time-decaying:** Enforcing continuous contribution
- **Publicly verifiable:** Transparent yet privacy-preserving
- **Domain-specific:** Specialized recognition with unified aggregation

7.2 Exponential Decay

The decay function emerges as the unique solution to prevent reputation hoarding while maintaining incentives for contribution.

$$R(t) = R_0 \cdot e^{-\lambda t} \tag{11}$$

This mathematical formulation prevents lifetime monopoly on influence by ensuring that past contributions, while valued, gradually diminish in weight relative to current efforts.

Domain-specific decay constants reflect knowledge velocity, calibrated from empirical data on citation half-lives, code repository activity patterns, and governance proposal lifecycles.

Example:

- Research: $\lambda = \ln(2)/6$ months (fast evolving field)
- Infrastructure: $\lambda = \ln(2)/24$ months (more rare because of resource intensity)
- Governance: $\lambda = \ln(2)/12$ months (stability balanced with renewal)

For half-life of 6 months:
$\lambda = \ln(2)/\text{half-life} = 0.693/6 \text{ months} \approx 0.116$ per month

See Appendix D.1 for domain specific parameters

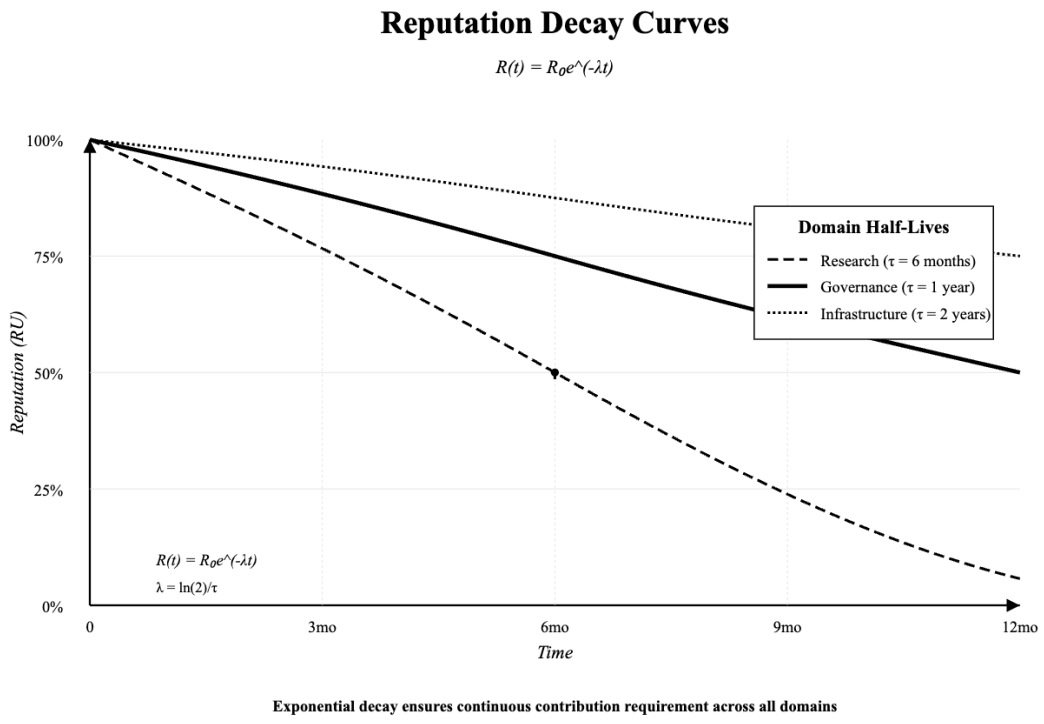

Figure 2: Reputation Decay Curves

7.3 Pseudonymous Support

The system explicitly supports pseudonymous contributors through:

- Contribution-based earning without identity disclosure
- Committee recognition of pseudonymous work
- Default treatment as non-wealthy ($W \leq W_{threshold}$)

RU Flows:

1. Contributor submits work under pseudonym
2. Domain committee evaluates contribution
3. RU minted to pseudonymous address
4. No wealth verification required
5. Default assumption: $W \leq W_{threshold}$

Edge Case: Malicious Anonymous Accumulation (manipulative agent)

Risk: Anonymous actor accumulates RU for later misuse

Mitigations:

1. Exponential decay requires continuous positive contribution
2. Governance actions logged publicly
3. Community can fork if captured
4. Slashing for proven malicious votes

Accepted Tradeoff: System prioritises permissionless contribution over perfect security.

This design choice accepts calculated risk: anonymous bad actors could accumulate RUs, but exponential decay provides natural defence.

7.4 Voting Mechanism

Voting power derives from total active reputation:

$$V(i) = f(\mathrm{RU}_{total}(i))$$

where $\mathrm{RU}_{total}(i) = \mathrm{UBR}(i) + \mathrm{RU}_{earned}(i) + \mathrm{RU}_{donated}(i)$

V(i) = f($\mathrm{RU}_{total}(i)$) where $f(x) = x$ (linear) or $f(x) = \sqrt{x}$ (quadratic)

$$V_{quadratic}(i) = \sqrt{\mathrm{RU}_{total}(i)}$$

Quadratic voting option further prevents dominance

8. Mathematical Foundations

8.1 Incentive Compatibility

Theorem 1. *For wealthy individuals ($W > W_{threshold}$), earning RU through contribution dominates donation strategies.*

Proof: See Appendix A.4

8.2 Convergence Properties

Theorem 2. *The system converges to equilibrium where reputation distribution reflects recent contribution patterns.*

Proof: See Appendix A.1

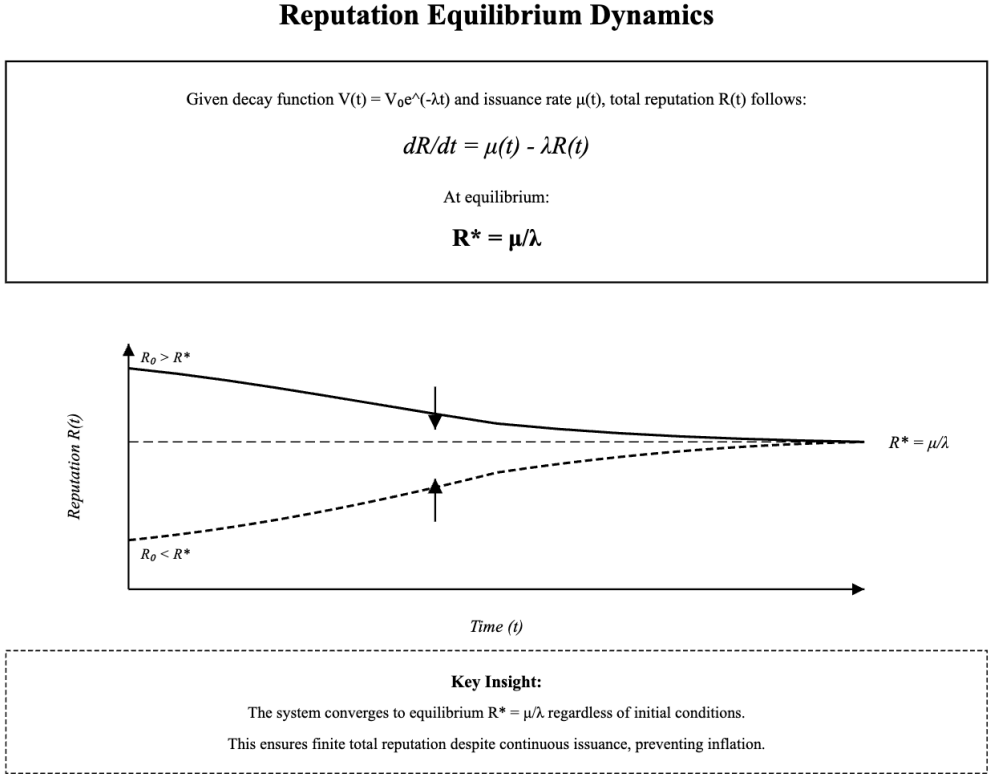

Figure 3: Reputation Equilibrium Dynamics

8.3 Sybil Resistance

Theorem 3: Given an external identity verification layer, the system's economic mechanisms target creating n identities to cost $O(n^2)$ while yielding reputation O(n).

The Sybil resistance mechanisms need to be flexible:

- For anonymous: Proof of work, time locks, resource bonding
- For verified: Economic stakes can work

We demonstrate an example in diagram below setting K = 20 RU & average RU earned = 100 RU

Proof: See Appendix A.2

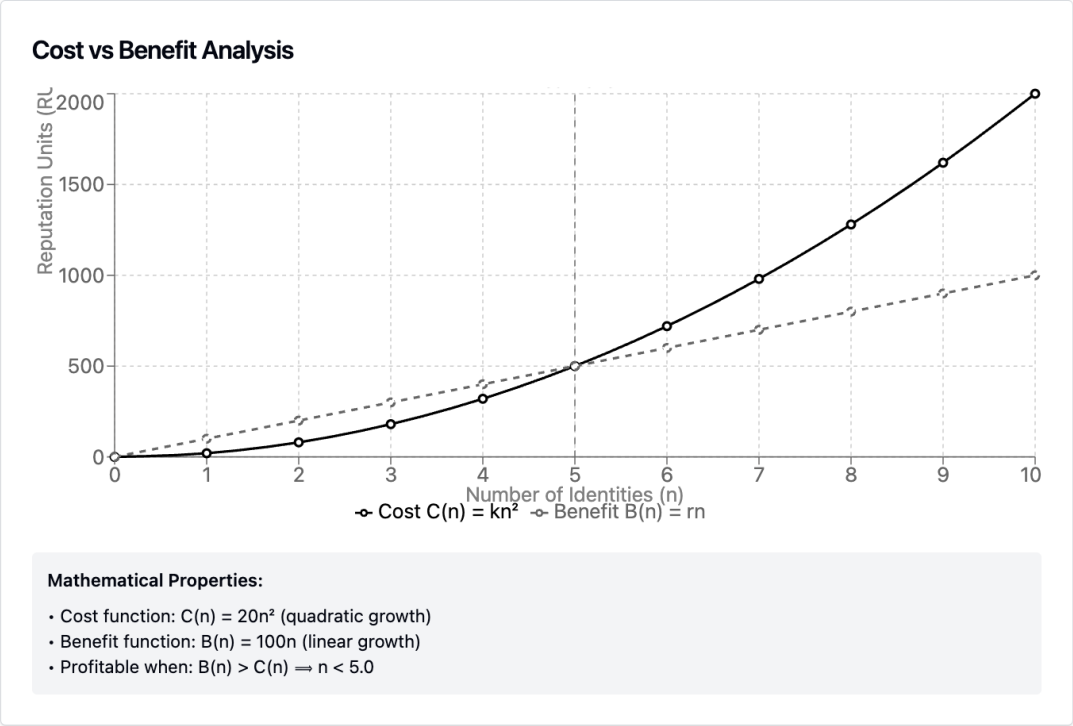

Figure 4: Sybil Attack Cost - Benefit Analysis

Note: K = 20 RU illustrates the quadratic cost mechanism. In practice, the system requires integration with real-world identity verification (e.g., India's Aadhaar, Estonia's e-Residency) as the primary Sybil defense. See Appendix A.2 for detailed analysis of identity mechanisms and pseudonymity tradeoffs.

9. System Architecture

9.1 Dual-Token Model

The system operates with two distinct tokens. RUs are non-transferable, individual bound, reputation markers that decay as per domain parameters. RCS are transferable utility tokens for network operations, staking, and validator incentives. This separation ensures reputation remains bound to individuals while allowing market dynamics for network resources.

Dual-Token Model

Token	Nature	Purpose
RU	Individual bound	Voting, governance, access rights
RCS	Transferable	Staking, fees, sponsorship

RU: Non-transferable reputation, governance, and access

RCS: Utility token for staking, compute, tip, AI-review fee

Figure 5: Dual-Token Model

9.2 Token Utility Mechanisms

Token Mechanisms and Dynamics

Circulation:
RUs: minted via verified events, decay ensures participation
RCS: rewards validators, provides network liquidity
Staking: Lock RCS to sponsor REE pools, earn fee share

Inflation & Tax:
RU Tax: 1-5% per epoch → UBI pool
RCS Emission: Controlled vesting to validator network

Reputation Staking (RU-based)	Economic Staking (RCS-based)
• For vouching for others' contributions	• For validator participation
• Risk of RU slashing if false claim	• Economic incentive alignment
• Non-transferable, reputation at risk	• Transferable tokens at stake

Figure 6: Token Mechanisms and Dynamics

9.3 System Integration Architecture

The protocol operates through seven interconnected layers, each providing essential services. The Identity Layer establishes decentralised identifiers and biometric anchors. The Contribution Input Layer accepts human and AI submissions. The Adjudication Layer implements AI triage and expert verification. The AI Oracle ensemble consists of multiple specialized models that assess contribution quality, detect plagiarism, verify impact claims, and flag potential manipulation, with human experts providing final validation for high-stakes or disputed contributions. The

RU Minting Layer creates tokens with appropriate metadata. The Decay Layer implements time-based depreciation. The Aggregation Layer calculates URI across domains. The Governance Layer enables voting and access control. The complete system architecture is illustrated in Figures 5-8, showing token flow, mechanisms, and layered design.

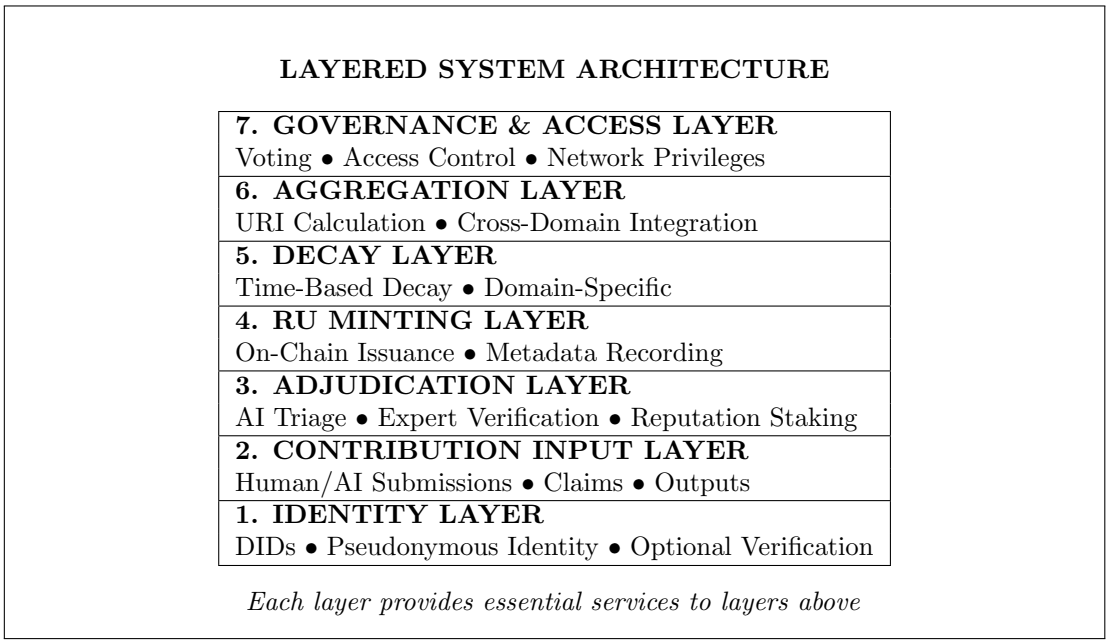

Figure 7: Layered System Architecture

9.4 Domain Integration

Domains maintain independent parameters specialised for each field's unique contribution patterns and verification requirements, while contributing to a Unified Reputation Index. Science values rapid iteration, infrastructure rewards longevity, governance balances stability with responsiveness. Each domain's weight reflects societal priorities, adjustable through governance. See Appendix D.1

9.5 Verification Protocol

Define concrete mechanisms for contribution impact measurement, Domain-specific verification criteria, AI-human adjudication process, Zero-knowledge proof construction.

10. Implementation Framework

10.1 Smart Contract Architecture

The RCS protocol implements through a system of interconnected smart contracts that enforce the mathematical and governance properties defined above. The core contracts handle RU

minting, decay calculation, verification attestation, and governance voting.

Technical Implementation details to be presented in subsequent works.

[Core RU Contract - Implements minting, decay, and aggregation]

[Voting Contract - Implements quadratic voting with RU weights]

[Wealth Adjustment Oracle - Implements donation adjustment calculations]

11. Economic Analysis

11.1 Nash Equilibrium

Given exponential decay, the optimal strategy becomes continuous contribution rather than hoarding. Accumulated reputation provides diminishing returns while fresh contributions maintain full value.

Mathematical proof demonstrates that for any finite reputation stock R, the value at time t equals $R_0 e^{-\lambda t}$, making new contribution of value C superior to old reputation R when $C > R_0 e^{-\lambda t}$.

The equilibrium state emerges where agents contribute at a rate that maximizes their long-term reputation value, accounting for decay. This creates a dynamic system where influence flows to those actively contributing rather than those resting on past achievements.

When accounting for coordination costs c, the equilibrium condition becomes: $\mu(r - c) = \lambda R^*$, where contribution rate μ adjusts to balance reward minus coordination cost against reputation decay.

11.2 Commons Amplification

Under RCS public goods receive multiplier $\alpha > 1$, contributing to public goods such as open source, public research, or community infrastructure yields higher individual returns than private accumulation, reversing traditional incentive structures where private gain is the dominant strategy.

The mathematical proof follows from the issuance formula where public good contributions receive $\alpha \times$ base_reward while private contributions receive only base_reward. Over time, the cumulative advantage of commons-oriented behavior dominates any short-term private gain strategy.

Let G be a contribution graph where public-good contributions receive $\alpha > 1$.
Long-term maximization of URI occurs via **communal acts**, not private gain. ■

11.3 Attack Resistance

Attack	Defense
Create fake identities	Real-world ID + ZK verification + economic deterrents
Spam small contributions	Diminishing returns + rate limits per epoch
Collude to verify fraud	Random validator selection + slashing
Buy reputation with money	Non-transferable + logarithmic resistance

- **Sybil attacks:** Quadratic identity costs
- **Wealth capture:** Logarithmic donation adjustment
- **Reputation hoarding:** Exponential decay

Sybil Attacks: The system's primary defense relies on integration with real-world identity verification systems (e.g., national digital IDs) that make obtaining multiple legitimate identities practically impossible, and optionally ZK proofs. Economic mechanisms like staking requirements and time delays serve as secondary deterrents. Without robust identity infrastructure, the protocol remains vulnerable to Sybil attacks regardless of economic costs. (See Appendix A.2)

Collusion Resistance: Collusion requires staking existing reputation that faces slashing upon detection, creating internal enforcement mechanisms. The stake-and-slash mechanism ensures that the expected value of collusion remains negative when detection probability exceeds the ratio of potential gain to staked reputation.

Wealth Capture: Logarithmic adjustment of donation-based reputation prevents direct translation of wealth into governance power (see Appendix A.4).

11.4 Wealth Adjustment Mechanism

The wealth adjustment mechanism ensures that while wealthy individuals can contribute meaningfully to the system, they cannot simply purchase influence. The logarithmic compression after the wealth threshold (set at \$100M) means that a billionaire must contribute exponentially more than a person of median wealth to earn the same reputation units.

11.5 Economic Benefits

RCS creates positive-sum dynamics through several mechanisms:

Commons Amplification: By rewarding public goods with multiplier $\alpha > 1$, RCS reverses the tragedy of the commons, making collective benefit individually rational.

Continuous Innovation: Exponential decay ensures economic rewards flow to active contributors rather than rent-seekers, maintaining system vitality.

Reduced Transaction Costs: Reputation-based coordination eliminates price discovery overhead in domains where pricing fails (public goods, innovation, community service).

Anti-Plutocratic: Logarithmic wealth adjustment prevents direct translation of capital into influence, creating more equitable governance.

Dynamic Equilibrium: The system naturally balances at $R^* = \mu/\lambda$, preventing both inflation and deflation of reputation currency. Ensures new reputation created replaces decaying reputation precisely, regardless of initial state.

11.5.1 Sensitivity Analysis

Monte Carlo simulations confirm system stability for $\lambda \in [0.5\lambda_0, 2\lambda_0]$.

11.6 Extended Game Theory Analysis

11.6.1 Contribution Game with Coordination Costs

Let r = reputation reward, c = coordination cost, λ = decay rate, R = current reputation.

Table 1: Payoff Matrix with Coordination Costs

	Others Contribute	Others Free-ride
Contribute	$r - c$	$r - c - \epsilon$
Free-ride	$-\lambda R$	$-\lambda R$

Theorem 3. *For $c < r + \lambda R - \epsilon$, contributing is the dominant strategy.*

Proof. If others contribute: $r - c > -\lambda R$ when $c < r + \lambda R$
If others free-ride: $r - c - \epsilon > -\lambda R$ when $c < r + \lambda R - \epsilon$
Therefore, contribute dominates for reasonable coordination costs. ■

11.6.2 Wealth Splitting Analysis

Theorem 4. *Wealth distribution across verified family members or friends increases individual RU for all parties, creating a controlled incentive for wealth distribution.*

Proof. Single concentrated wealth: $RU_1 = \beta \times D \times \frac{\log(1+W_{threshold})}{\log(1+W)}$

Distributed wealth: Each member i receives $RU_i = \beta \times D \times \frac{\log(1+W_{threshold})}{\log(1+W_i)}$

Since $W_i < W$ for all i: $RU_i > RU_1$ for each family member, including the original wealth holder.

Accepted Trade-off: While this creates an incentive to distribute wealth among family (similar to current tax optimization strategies), this is philosophically aligned with RCS goals:

- Encourages wealth distribution vs concentration
- Each identity requires real verification (cost β)
- System correctly reflects reduced individual wealth holdings
- Prevents plutocratic capture while allowing legitimate family wealth strategies

This represents an intentional design feature that mirrors real-world wealth distribution patterns.See Appendix F for implementation notes on wealth disclosure mechanisms. ■

12. Governance

12.1 Voting Power Distribution

$$V = \sqrt{\text{URI}} \times \text{activity\_modifier} \times \text{domain\_weight}$$

Voting weight equals $\sqrt{\text{URI}}$, compressing power differentials while maintaining meritocratic influence. This quadratic voting mechanism prevents both mob rule and oligarchic capture while rewarding active participation. The square root function ensures that while higher reputation grants more influence, the relationship is sub-linear, preventing excessive concentration of power. No individual can accumulate overwhelming influence regardless of reputation magnitude.

12.2 Domain Councils

Domain councils manage parameters through reputation-weighted governance, with changes requiring 66% supermajority for protocol modifications and 51% for operational decisions. Each domain maintains autonomy over its specific parameters while coordinating through the unified governance layer for system-wide changes.

12.3 Dispute Resolution

Dispute resolution follows stake-and-challenge protocols. Challengers stake reputation against claims, with successful challenges earning rewards and false challenges facing slashing. This creates market dynamics for truth discovery without central arbitration. The mechanism ensures that the cost of false challenges exceeds potential gains from successful attacks on legitimate contributions.

13. Limitations and Open Questions

While RCS provides a theoretical framework for post-scarcity coordination, several challenges require acknowledgment:

13.1 Implementation Challenges

Sybil Resistance: True Sybil resistance requires integration with real-world identity verification systems, which inherently introduces some centralization. The theoretical $O(n^2)$ cost function and RU cost for pseudonymous identities provides only secondary protection and cannot serve as the primary defense against Sybil attacks in a fully decentralized system.

Verification Infrastructure: The multi-layer verification system requires sophisticated AI and human coordination that may initially limit scalability.

Privacy-Verification Tradeoff: Zero-knowledge proofs for contribution verification while maintaining pseudonymity present technical complexity.

The protocol envisions zkSNARK circuits that prove: (1) contribution ownership, (2) impact threshold met, (3) no double-claiming, without revealing contributor identity. The system's effectiveness depends critically on empirical parameter tuning:

Decay rates (λ) must balance knowledge velocity with participation incentives.

Commons multipliers (α) require careful calibration to prevent gaming.

Wealth thresholds need regular adjustment for economic conditions.

Resource Scarcity: While goods become abundant, attention and verification resources remain scarce. The protocol assumes sufficient participants willing to verify contributions, which may require incentive calibration during deployment.

13.2 Potential Failure Modes

Coordination Failures: If too few participants adopt the system, network effects may fail to materialize

Gaming Vulnerabilities: Sophisticated actors may discover exploits in the verification or decay mechanisms

Governance Capture: Despite quadratic voting, coordinated minorities might influence parameter decisions

Cultural Resistance: Societies with different values around contribution and reputation may reject the framework

The following require rigorous testing and emperical validation before deployment:

Optimal decay constants for different domains

Effectiveness of proposed Sybil resistance mechanisms

Behavioral responses to reputation incentives

Cross-cultural validity of contribution metrics

These limitations do not invalidate RCS but highlight areas requiring continued research and iterative refinement.

14. The Reputation Circulation Standard - Conclusion

In the absence of scarcity, price ceases to coordinate.

Artificial intelligence collapses the marginal cost of labor. Markets, once driven by capital allocation, no longer align incentives or signal value. Traditional economic primitives—money, ownership, accumulation—fail to sustain cooperation or legitimacy.

The Reputation Circulation Standard defines reputation as a nontransferable, time-decaying proof of contribution: $R(t) = R_0 \cdot e^{-\lambda t}$

This introduces a perishable coordination substrate, where influence reflects ongoing participation, not possession. Each Reputation Unit encodes verified contribution—a *Proof-of-Impact*. Reputation decays unless renewed. Accumulation becomes unsustainable. Static authority becomes unstable equilibrium.

Governance becomes a function of recent, verifiable alignment. It preserves incentive coherence without relying on price. The protocol constructs a system where contribution governs access, renewal enforces persistence, verification ensures legitimacy, and plutocracy is unsustainable. Wealth adjustment and quadratic voting limit reputation farming and structurally resist capture. **The tragedy of the commons becomes economically irrational.**

A Universal Basic Reputation allows all to retain dignity, and UBI pools are replenished with voluntary donations, and protocol tax on the reputation wealthy. Through commons amplification and wealth adjustment, RCS creates an equilibrium where contribution dominates extraction, where public benefit yields private gain, where governance flows only to those who continue to build, and moral hazard is structurally minimised. Reputation decay solves currency for post-scarcity coordination.

As artificial minds surpass human capability, what remains distinctly human is not what we can do, but what we choose to value. When machines execute anything we can describe, the sole domain that remains ours is the authorship of what should be. Our imagination.

In an economy of unbounded creation, the ultimate act becomes specification: the ability to define what matters, to derive meaning, to determine the trajectory of our post-scarcity civilisation. The locus of agency shifts from doing to deciding, from production to purpose.

Artificial intelligence can be coopted to this game of cooperation. The protocol admits human and non-human agents, free to earn reputation across domains. Where capital once governed access, contribution becomes the new substrate of coordination.

A law of decay, applied to reputation, becomes the immune system of civilization—preserving human agency, even as our tools surpass us.

Through the mathematics of decay, RCS instates the fundamental law of change:

Nothing persists without continued relevance.

This law—which governs collective human memory, power, and meaning—through RCS, governs coordination itself.

RCS offers a concrete architecture for post-scarcity coordination, where contribution rather than capital governs influence.

15. References

1. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
2. Ostrom, E. (1990). Governing the Commons. Cambridge University Press.
3. Nash, J. (1951). Non-Cooperative Games. Annals of Mathematics.
4. Hardin, G. (1968). The Tragedy of the Commons. Science.
5. Weyl, E. G., Posner, E. A. (2018). Radical Markets. Princeton University Press.
6. Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. First Monday, 2(9).

Appendices

A. Mathematical Foundations

A.1 Exponential Decay Equilibrium

Theorem 2: The system converges to equilibrium where reputation distribution reflects recent contribution patterns.

Proof: Given decay function $R(t) = R_0 e^{-\lambda t}$ and issuance rate $\mu(t)$, total reputation $R(t)$ follows:

$$\frac{dR}{dt} = \mu(t) - \lambda R(t)$$

At equilibrium: $R^* = \mu/\lambda$

$$R(t) = R_0 e^{-\lambda t} + \frac{\mu}{\lambda}(1 - e^{-\lambda t})$$

As $t \to \infty$: $\lim_{t\to\infty} R(t) = \mu/\lambda$

At steady state, issuance equals decay: $\partial R/\partial t = \mu - \lambda R = 0$, yielding equilibrium $R^* = \mu/\lambda$. This ensures finite total reputation despite continuous issuance. Any initial state R_0 converges to R^* as $t \to \infty$. ■

A.2 Sybil Resistance Design

Theorem 3: Under implementation-specific identity verification mechanisms, the system can achieve economic Sybil resistance where attack profitability diminishes with scale.

Proof: Let $C(n)$ be the cost function for creating n identities and $G(n)$ be the reputation gain. Economic resistance requires $C(n)/G(n)$ to be increasing with n. For proposed mechanisms:

1. Quadratic staking: $\text{Stake}(n) = \text{base\_stake} \times n^2$
2. Escalating proof-of-work: $\text{Difficulty}(n) = \text{base\_difficulty} \times f(n)$ (each additional identity requires solving puzzles of quadratically increasing computational difficulty)
3. Time locks / delays: $\text{Wait}(n) = \text{base\_time} \times g(n)$

Where $f(n)$ and $g(n)$ are increasing functions chosen to make $C(n) \geq kn^\alpha$ for $\alpha > 1$.

With linear reputation gain $G(n) \leq rn$, profitability requires:

$$C(n) < G(n) \to kn^\alpha < rn \to n < (r/k)^{1/(\alpha-1)}$$

For $\alpha = 2$ (quadratic costs), break-even occurs at $n = r/k$.

Critical Assumption: Actual resistance depends on successful implementation of super-linear cost mechanisms, which face practical challenges in decentralized systems.

Economic Analysis: If mechanisms achieve target cost function $C(n) = kn^2$

Reputation gain: $G(n) \leq rn$ (best case)

Break-even: $kn^2 = rn \rightarrow n = r/k$; for $n > r/k$, attack becomes unprofitable

Result: The quadratic cost model assumes pre-existing identity verification infrastructure. In jurisdictions with robust digital identity systems, creating $n > 1$ verified identities is practically impossible, making the economic model relevant only for deterring multiple pseudonymous identities. Without such infrastructure, the economic mechanisms alone cannot prevent Sybil attacks, as attackers can create unlimited "first" identities at insignificant cost (designed to be inclusive to onboard everyone).

A.2.1 Identity Verification and Pseudonymity

The system implements a two-tier identity model:

1. Verified identities: One per person via real-world identity infrastructure, receiving 100 RU UBR upon verification, for example.

2. Pseudonymous identities: Require staking 500 RU to create.

This creates an inherent tension: since RU is non-transferable and on-chain traceable, accumulating 500 RU for pseudonymous identity creation inherently creates linkages that may compromise anonymity. Whether through direct contribution (linking achievements) or donations (creating social traces), the qualification process itself generates identifying information.

This paradox parallels Bitcoin's pseudonymity model - technically private but practically traceable through transaction analysis. The high RU threshold ensures only those with genuine privacy needs accept these tradeoffs. How truly anonymous identities might emerge - through operational security, time delays, or other strategies - remains an open implementation question.

The quadratic cost function $C(n) = kn^2$ applies only to creation of multiple identities beyond the first, serving as an additional economic deterrent rather than primary defense. True attackers will avoid this path.

A.3 Wealth Resistance Limit

As $W \rightarrow \infty$, $\partial \text{RU}/\partial D \times (1/W) \rightarrow 0$, ensuring wealth cannot purchase unlimited influence regardless of contribution size. The logarithmic adjustment ensures that even infinite wealth cannot overcome the fundamental requirement for genuine contribution to earn reputation.

A.4 Wealth Adjustment Optimality

Theorem 1: For wealthy individuals ($W > W_{threshold}$), earning RU through contribution is more efficient than through donation.

Proof: Let C = contribution effort cost, D = donation amount, W = individual wealth where $W > W_{threshold}$.

For contributions: where f(contribution quality, domain) is independent of contributor wealth by design

$$\text{RU(contribution)} = \alpha \times C \times f(\text{contribution\_quality}, \text{domain})$$

For donations:

$$\text{RU(donation)} = \beta \times D \times \frac{\log(1 + W_{threshold})}{\log(1 + W)}$$

As $W \to \infty$:

$$\lim_{W \to \infty} \frac{\text{RU(donation)}}{D} = \beta \times \frac{\log(1 + W_{threshold})}{\log(1 + W)} \to 0$$

While RU(contribution) remains constant with respect to wealth.

Therefore, $\exists W^*$ such that $\forall W > W^*$: RU(contribution)/C > RU(donation)/D ■

B. Smart Contract Specifications

The core contracts presented in Section 5 demonstrate the fundamental mechanics while production deployment would require contracts for governance voting, domain management, and oracle integration, additional security features, upgrade mechanisms, and integration points.

Key interfaces include IRU for reputation queries, IGovernance for voting mechanisms, and IOracle for external verification integration. The modular design allows for protocol upgrades while maintaining backward compatibility with existing reputation holdings.

C. Implementation Parameters

C.1 Technical Requirements

Core Infrastructure requirements include zero-knowledge proof systems for privacy-preserving verification, distributed ledger with smart contract capability, AI verification ensemble with fraud detection, and high-throughput consensus mechanism supporting 10,000+ TPS.

We suggest design targets of verification completion within 24 hours, RU minting within 1 minute

of verification, query response under 100ms, and system scale to 1 billion users with 100 million daily contributions.

D. Configuration Parameters

These parameters are illustrative examples. Actual values must be determined through: Community-specific economic modeling, empirical observation of user behavior, and iterative adjustment based on system performance.

D.1 Domain-Specific Parameters

The commons multiplier α should satisfy: $\alpha > 1$ (incentivizes public goods) $\alpha < (1 +$ median_contribution_rate) (to prevent gaming)

Commons multiplier $\alpha \in [1.5, 2.5]$ - higher values incentivize public goods but risk gaming.

Domain	**Suggested Half-Life**	**Decay Constant (λ)**	**Reasoning**
Research	6-12 months	0.116-0.058/month	Rapid innovation cycles
Infrastructure	18-36 months	0.039-0.019/month	Stable technical requirements
Governance	9-15 months	0.077-0.046/month	Balance stability with renewal

The values of (λ) are calculated as: (λ) = ln(2) / half-life = 0.693 / half-life;

For 6 months: (λ) = 0.693/6 = 0.116/month; For 12 months: (λ) = 0.693/12 = 0.058/month calibrated from empirical data on citation half-lives

D.2 System Constants

Parameter	**Value**	**Rationale**
Wealth Threshold	$100M	Diminishing utility point
Base UBR	100 RU	Ensures participation floor
Design Sybil Cost Factor	k	to make attacks uneconomical

Sybil Defense Factor β = max(100 RU, AttackProfit/IDCost); Economic deterrent calibration

Note: The example in Section 8.3 demonstrates the mechanism with k = 20 for illustration purposes. As discussed in Appendix A.2, The production value k provides stronger security guarantees only for known identities that are already in the system, not new attackers.

Anti-Sybil Calibration

From the economic analysis (Appendix A.2):

Suggested: Set $k = r$/target_identities; where target_identities = acceptable Sybil threshold

(typically 3-5). Example: If $r = 100$ RU and target = 5, then $k = 20$ RU

Monitor and adjust based on: Observed attack attempts, Network growth rate, Economic conditions

D.3 Wealth Adjustment Threshold

The threshold $W_{threshold}$ should approximate the wealth level where: Marginal utility of additional wealth significantly decreases

Political influence through traditional channels plateaus, for example

Suggested heuristics: Developed economies: 100-1000× median wealth - $50-100M

Emerging economies: 50-500× median wealth, may need regional adjustments

Requires periodic adjustment for inflation and wealth distribution changes

D.4 Voting Parameters

These are illustrative parameters. Actual values require empirical calibration based on: Community size and activity levels, economic modeling of incentives, observed attack patterns

Mechanism	**Formula**	**Use Case**
Linear	$V = \text{RU}_{total}$	Standard decisions, routine operations, simple & intuitive
Quadratic	$V = \sqrt{\text{RU}_{total}}$	Constitutional changes; High-stakes governance; prevents dominance
Capped	$V = \min(\text{RU}_{total}, \text{cap})$	Emergency protocols, crisis response, ensures broad participation. Suggested cap: $\mu + 2\sigma$ where μ = mean RU holdings, σ = std deviation

D.5 Parameter Design Guidelines

1. **Decay Rate (λ):** Choose based on domain knowledge velocity
   - Fast-moving fields: $\lambda \approx \ln(2)/6$ months
   - Stable fields: $\lambda \approx \ln(2)/24$ months
2. **Wealth Threshold:** Set at level where diminishing utility begins
   - Suggested: 100× median wealth in community
3. **Commons Multiplier (α):** Balance individual vs collective incentive
   - Min: $\alpha > 1$ to incentivize public goods

- Max: $\alpha < 3$ to prevent gaming

D.5.1 Empirical Calibration of Decay Parameters

Drawing from empirical data across multiple domains:

Research Domain ($\lambda = 0.116$/month)

- Based on computer science citation half-life: 6-8 months
- GitHub repository star decay: 50% activity loss in 6 months
- arXiv paper attention span: 90% of views within 6 months

Infrastructure Domain ($\lambda = 0.029$/month)

- Software depreciation studies: 2-3 year useful life
- npm package maintenance cycles: 24-month average
- Critical infrastructure update cycles: 18-36 months

Governance Domain ($\lambda = 0.058$/month)

- Political term limits: 2-6 years globally
- DAO proposal relevance: 12-month average
- Corporate board turnover: 15% annually

Note: Empirical validation through pilot implementations recommended before full deployment.

E. Implementation Notes on Wealth Disclosure

E.1 Wealth Verification Challenges

The $W_{threshold}$ mechanism faces several practical implementation challenges:

1. **No reliable wealth verification mechanism** – Unlike income (W-2 forms) or specific assets (property records), total wealth remains opaque due to complex ownership structures, trusts, and offshore entities.
2. **Self-reporting with social accountability** – The system relies on self-reported wealth subject to public scrutiny. Public figures face reputational constraints on false claims (e.g., Elon Musk claiming net worth below $100M would face immediate public ridicule).
3. **Universal optimization behavior** – Rational actors will claim $W < W_{threshold}$ to maximize RU per donation, similar to tax optimization strategies.

E.2 Equilibrium Dynamics

This creates a natural equilibrium where:

- Most contributors claim $W < W_{threshold}$ (maximizing RU per donation)
- Obviously wealthy individuals face social pressure for honest disclosure
- Family distribution becomes optimal strategy for wealthy participants
- Even above threshold, RU continues to accrue at reduced rate: $\frac{d(RU)}{dD} > 0$ for all W

E.3 Accepted Trade-offs

The "loophole" of family wealth distribution achieves several design objectives:

1. Incentivizes wealth distribution over concentration
2. Mirrors existing tax optimization behaviors (familiar paradigm)
3. Maintains contribution incentives even for wealthy participants
4. Creates social pressure for appropriate wealth disclosure

These dynamics represent acceptable trade-offs that align with the system's philosophical goals of preventing plutocratic capture while maintaining practical implementability.

The Reputation Circulation Standard represents a fundamental reimagining of economic coordination for the post-scarcity era. By establishing reputation as a formal economic primitive with mathematical properties that enforce continuous contribution, RCS provides the coordination layer necessary for a civilization where traditional price mechanisms no longer function. This paper presents the core protocol, leaving implementation details and policy implications for subsequent work.

sha256 9fb23414a61dad2de92b3e36e3057da74eb84d234809dee7cc047139b53d842e

created 2 Aug 2025

https://deepthinker.xyz

https://deepthinker.xyz/papers/RCS-v1.pdf