The DRanking Protocol:

Verifiable Distributed Ranking and Sybil-Bounded Admission
for Structured Peer-to-Peer Networks

Ryan J. Kung*

Abstract

DRanking converts locally observed peer behavior in an open structured peer-to-peer network into a globally agreed, verifiable service weight that gates admission to protocol roles. Identity creation is free, so no mechanism bounds adversarial *count* [1]; the protocol instead bounds adversarial *weight* and prices it. The instruments are: counterparty-signed service receipts in place of unsigned counters; a seed-anchored trust flow $t_{k+1} = \alpha C_k^{\mathsf{T}} t_k + (1-\alpha)s$ obeying conservation, attenuation, and revocation laws, with a proved bound $T_k(A) \leq \alpha g/(1-\alpha)$ on Sybil mass; trust-weighted verifiable random sortition in place of oracle sampling; a proof-of-authority ledger trusted for ordering only, with equivocation proofs as first-class slash objects; and a circuit-friendly epoch transition folded by Nova-family incrementally verifiable computation, giving constant-cost verification to browser nodes. Rank is soulbound and slashable; reward is a separate transferable asset; the authority-to-stake transition is conditioned on a security-budget crossover.

Keywords: peer-to-peer networks; service receipts; trust propagation; Sybil resistance; verifiable computation.

Implementation scope. Rings 1.0 [2] establishes the cryptographic identity, session delegation (`rings-delegation-v1`), and counterparty-signed service receipt (`rings-service-receipt-v1`) primitives on the wire. This paper specifies the complete Rings 2.0 decentralized trust, Sybil-resistant PageRank/EigenTrust propagation, verifiable random sortition, and Nova-folded admission layer built directly atop those 1.0 primitives. See the repository's service-receipt documentation.

1 Introduction

The 2023 draft of this protocol scored behavior per identity. Identities are free; every component secured against lying nodes fell to numerous nodes. This rewrite keeps the draft's decomposition — local evidence, global aggregation, sampling, ledger, incentives — and replaces the quantity being secured:

$$\begin{aligned} \mathsf{cost}(\mathsf{did}) &= 0, \\ |\mathsf{Adv} \cap V| &\leq \infty, \\ \mathsf{secure}(|\cdot|) &= \bot \quad [1], \\ \mathsf{secure} &:= \mathsf{secure}(T(\cdot)), \\ T(A) &= \textstyle\sum_{v \in A} t(v), \\ \mathsf{claim} &= \mathsf{price}\big(T(\mathsf{Adv}) \geq \tfrac{1}{3}\big). \end{aligned}$$

Sections 2–9 construct t, its evidence, its sampling, its ledger, and its economy; Section 10 tabulates the attack surface. Each mechanism is a term of price.

*Ryan J. Kung can be reached at ryankung@ieee.org. Manuscript created February 11, 2023; rewritten August 31, 2026; revised September 1, 2026. This document supersedes the 2023 draft *The Ranking Protocol*.

2 Model

Definition 1 (Substrate)**.**

$$\begin{aligned} R &= \mathbb{Z}/2^{160}\mathbb{Z} \quad \textit{[3, 4]}, \\ \mathsf{did} &: K \to R, \quad \textit{self-certifying}, \\ \mathsf{link} &\subseteq V \times V, \quad \textit{authenticated}, \\ \mathsf{msg} &= \langle m, \sigma_{\mathsf{origin}} \rangle, \\ \mathsf{cost}(\mathsf{did}) &= 0, \\ \mathsf{cost}(\mathsf{link}) &= \varepsilon > 0. \end{aligned}$$

Definition 2 (Epoch)**.**

$$\begin{aligned} k \in \mathbb{N}, \qquad \mathsf{epoch}(k) &= [\,\mathsf{fin}(\Sigma_k),\ \mathsf{fin}(\Sigma_{k+1})\,), \\ \mathsf{close}(k) \equiv \mathsf{elapsed} \geq T_{\mathrm{ep}} &\quad \textit{(proposer duty)}, \end{aligned}$$

delimited by ledger finality (Definition 11); the timer T_{ep} is what enables Next *in Section 8.*

Assumption 1 (Adversary)**.**

$$\begin{aligned} |\mathsf{Adv}| &\leq \infty, \\ \mathsf{collude},\ \mathsf{grind},\ \mathsf{patience} &\in \mathsf{Cap}(\mathsf{Adv}), \\ \mathsf{byzantine} &\in \mathsf{Cap}(\mathsf{Adv}), \\ \mathsf{forge}(\sigma_h),\ h \notin \mathsf{Adv} &\notin \mathsf{Cap}(\mathsf{Adv}), \\ \mathsf{break}(\mathsf{VRF}) &\notin \mathsf{Cap}(\mathsf{Adv}). \end{aligned}$$

Assumption 2 (Honest weight)**.**

$$T_k(\mathsf{Adv}) \ < \ \tfrac{1}{3}\, T_k(V) \qquad \forall k.$$

No bound is assumed on $|\mathsf{Adv}|$.

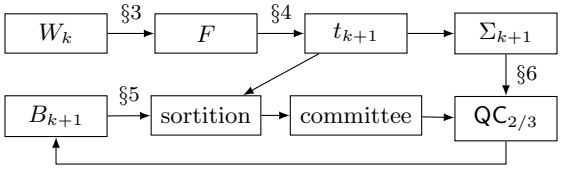

Figure 1: Epoch cycle: receipts fold into trust, trust seats the committee, the committee finalizes the ledger and threshold-signs the beacon.

3 Service Receipts

Unsigned counters are first-person testimony; aggregated, they are hearsay. The unit of evidence is a countersigned receipt.

Definition 3 (Receipt)**.**

$$\rho = \langle \mathsf{srv}, a, b, k, n, \sigma_b \rangle,$$

$$\begin{aligned} \mathsf{srv} &\in \{\mathsf{relay}, \mathsf{store}, \mathsf{probe}\}, \\ a &= \textit{server}, \quad b = \textit{signer/served}, \\ \mathsf{valid}(\rho) &\equiv \mathsf{Vrfy}(k_b, \sigma_b, \mathsf{srv}\|a\|b\|k\|n) = \top \\ &\quad \wedge\ (b, k, n)\ \textit{fresh within}\ P_k, \end{aligned}$$

freshness scoped to the epoch-k input block P_k (Definition 12): the tuple carries k, so no cross-epoch nonce state exists.

Proposition 1 (Forgery surface)**.**

$$\mathsf{valid}(\rho) \wedge b \notin \mathsf{Adv} \ \Rightarrow\ \rho\ \textit{issued by}\ b.$$

Proof. Immediate from $\mathsf{forge}(\sigma_b) \notin \mathsf{Cap}(\mathsf{Adv})$ (Assumption 1). Manufacturable receipts are exactly those with $b \in \mathsf{Adv}$ (self-dealing); these are neutralized by signer-trust weighting (Section 4). □

Definition 4 (Receipt graph)**.**

$$\begin{aligned} \mathsf{val}(\rho) &= \mu_{\mathsf{srv}(\rho)} \cdot \mathsf{units}(\rho), \quad \mu\ \textit{published per kind}, \\ W_k &\in \mathbb{R}_{\geq 0}^{V \times V}, \\ W_k[b, a] &= \textstyle\sum\{\mathsf{val}(\rho) : \rho\ \textit{valid},\ \mathsf{sig}\ b,\ \mathsf{srv}\ a,\ \mathsf{ep}\ k\}, \\ W_k[b, \cdot]\,\mathbf{1} &\leq w_{\max}. \end{aligned}$$

The cap makes countersigning a budgeted act; the protocol certifies performed service, never synthetic load (cf. Constraint 1).

Rings 1.0 cryptographic foundation and 2.0 progression. Rings 1.0 [2] ships the foundational countersigned service-receipt primitive (`rings-service-receipt-v1`), signed by distinct provider and beneficiary account roles over a domain-separated transcript binding the overlay identifier, epoch, fresh nonce, and the digests of the exact signed request and completion transactions, with separated live collection and cryptographic verification predicates and bounded local evidence retention. Rings 2.0 lifts these 1.0 counterparty-signed receipts directly into finalized input blocks P_k (Definition 12), activating global receipt-graph aggregation W_k, seed-anchored trust propagation, trust-weighted VRF committee sortition, and Nova-folded ledger finality.

4 Trust Algebra

Definition 5 (Seed vector)**.**

$$\begin{aligned} s &\in [0, 1]^V, \qquad \textstyle\sum_v s_v = 1, \\ \mathsf{supp}(s) &= S \quad \textit{(authority set).} \end{aligned}$$

Law 1 (Conservation)**.**

$$C_k[b, a] = \frac{W_k[b, a]}{\max\big(w_{\max},\ W_k[b, \cdot]\,\mathbf{1}\big)}, \qquad C_k[b, \cdot]\,\mathbf{1} \leq 1.$$

Law 2 (Attenuation)**.**

$$\alpha \in (0, 1), \qquad \mathsf{flow}(\ell\ \textit{hops}) \leq \alpha^{\ell}.$$

Law 3 (Revocation)**.**

$$\begin{array}{rcl} \mathsf{slash}(v) & \Rightarrow & v \notin \mathsf{carrier}: \ v \text{ is excluded from} \\ & & \text{the vector, the columns and rows} \\ & & \text{of } C, \text{ and the seed vector } s, \\ t_{k+1} & = & f(W_k, t_k) \quad \text{(re-derived per epoch)}, \\ s\restriction_{V\setminus\mathsf{sl}} & & \text{un-renormalized: a slashed seed's} \\ & & \text{share burns; re-endorsement is a} \\ & & \text{threshold op (Def. 9).} \end{array}$$

Without the column and seed restrictions the slash is cosmetic: receipts naming v as server, or a fixed $s_v > 0$, would re-grant mass to v one epoch later.

Definition 6 (Trust update)**.**

$$t_{k+1} = \alpha\, C_k^{\mathsf{T}} t_k + (1-\alpha)\, s. \tag{1}$$

One power-iteration step per epoch toward $t^* = (1-\alpha)(I - \alpha C^{\mathsf{T}})^{-1} s$ [5, 6]; the fixpoint is approached along chain time, never computed within an epoch (cf. Definition 14).

Invariant 1 (Mass)**.**

$$\textstyle\sum_v t_0(v) = 1 \;\Rightarrow\; \sum_v t_k(v) \le 1 \quad \forall k.$$

Proof.

$$\begin{aligned} \textstyle\sum_v t_{k+1}(v) &= \alpha\, \mathbf{1}^{\mathsf{T}} C_k^{\mathsf{T}} t_k + (1-\alpha) \\ &\le \alpha\, \mathbf{1}^{\mathsf{T}} t_k + (1-\alpha) \quad \text{(Law 1)} \\ &\le \alpha + (1-\alpha) = 1 \quad \text{(induction)}. \end{aligned}$$

□

Proposition 2 (Sybil influence bound)**.** *Partition $V = H \uplus A$, $S \subseteq H$. Let*

$$g_k = \sum_{b\in H,\, a\in A} C_k[b,a]\, t_k(b), \qquad g = \sup_k g_k.$$

Then

$$T_k(A) = \sum_{v\in A} t_k(v) \;\le\; \frac{\alpha\, g}{1-\alpha} \qquad \forall k.$$

Proof. $S \cap A = \varnothing$ kills the seed term over A. Splitting (1) by origin region and applying Law 1 to internal circulation,

$$T_{k+1}(A) \le \alpha\big(g_k + T_k(A)\big).$$

From $T_0(A) = 0$,

$$T_k(A) \le \alpha g \sum_{i\ge 0} \alpha^i = \frac{\alpha g}{1-\alpha}.$$

□

$T(A)$ is linear in honest endorsement granted (g), independent of $|A|$. Defense concentrates on g: endorsement spends budget (Law 1), and detection claws it back (Law 3).

Proposition 3 (Farming price)**.** *Instantiating Proposition 2 at $A = \{v\}$: sustaining weight w requires per-epoch honest endorsement*

$$g_v \;\geq\; \frac{1-\alpha}{\alpha}\, w \qquad \textit{for every epoch the weight is held,}$$

so

$$\mathsf{farm}(w, \ell \textit{ epochs}) \;\geq\; \ell \cdot \mathsf{cost}\Big(\tfrac{1-\alpha}{\alpha}\, w\Big) \;+\; \Pr[\mathsf{detect}] \cdot u(w),$$

where $u(w)$ is the holder's valuation of the forfeited stock (same cost units as the first term); the second term by Law 3: one accepted equivocation forfeits the stock. This is the farm *function of Proposition 14, made explicit.*

Proof. $T_k(\{v\}) \leq \alpha g_v/(1-\alpha)$; rearrange, multiply by holding duration, add the slash expectation. □

Proposition 4 (Geometric convergence)**.** *For stationary $C_k = C$, the map $\Phi(x) = \alpha C^{\mathsf{T}} x + (1-\alpha)s$ satisfies*

$$\|\Phi(x) - \Phi(y)\|_1 \leq \alpha \|x - y\|_1,$$

hence t^* is the unique fixpoint and

$$\|t_k - t^*\|_1 \;\leq\; \alpha^k \, \|t_0 - t^*\|_1.$$

Proof.

$$\begin{aligned} \|C^{\mathsf{T}}(x-y)\|_1 &= \textstyle\sum_a \big|\sum_b C[b,a](x_b - y_b)\big| \\ &\leq \textstyle\sum_b \big(\sum_a C[b,a]\big)|x_b - y_b| \leq \|x - y\|_1 \end{aligned}$$

by Law 1; Banach on the affine contraction. Under drifting C_k the iterate tracks the moving fixpoint with lag $O(\alpha^j)$ per j epochs of stability. □

Definition 7 (Soulbound rank)**.**

$$\begin{array}{rcl} \mathsf{rank}_k(v) & = & t_k(v), \\ \mathsf{transfer} & \notin & \mathsf{Ops}(\mathsf{rank}), \\ \mathsf{rank} & \xrightarrow{\mathsf{slash}} & 0, \\ \mathsf{rank} & \xrightarrow{\mathsf{epoch}} & \textit{re-derived } (1). \end{array}$$

(Cf. Proposition 14.)

Definition 8 (Dilution schedule)**.**

$$\begin{array}{rcl} \mathsf{vol}_k & = & \sum_{i \leq k} \mathbf{1}^{\mathsf{T}} W_i \, \mathbf{1}, \\ 1 - \alpha_k & = & D(\mathsf{vol}_k), \quad D \textit{ non-increasing, published}, \\ \bar{\alpha} & = & \sup_k \alpha_k \;<\; 1, \\ t_0 & = & s \quad \textit{(cold start)}. \end{array}$$

Propositions 2–4 hold under the time-varying schedule with $\alpha := \bar{\alpha}$.

Definition 9 (Threshold authority)**.**

$$\begin{array}{rcl} \mathsf{Ops}(S) & = & \{\mathsf{withdraw}, \mathsf{rotate}, \\ & & \quad \mathsf{endorse}_0, \mathsf{reshare}\}, \\ o \in \mathsf{Ops}(S) & \Rightarrow & \mathsf{QC}_\theta(S)(o), \quad \theta \geq \tfrac{2}{3}, \\ |\mathsf{comp}| < \theta|S| & \Rightarrow & \mathsf{Cap}(\mathsf{Adv}) \cap \mathsf{Ops} = \varnothing, \\ \mathsf{keys} & : & \textit{genesis DKG;} \ \mathsf{rotate} \ \textit{and} \\ & & \textit{beacon-group change trigger} \\ & & \textit{proactive} \ \mathsf{reshare}, \\ & & \textit{preserving} \ \mathsf{gpk}. \end{array}$$

5 Sortition

Proposition 5 (Statistical undetectability)**.** *Model* $\mathsf{did} = \mathsf{h}(\mathsf{pk})$*,* h *a random oracle. For the adversarial placement strategy "sample fresh keys," honest and adversarial positions are identically distributed on* R*:*

$$\Delta_{\mathrm{TV}}\big(\mathsf{pos}(H \uplus A),\ \mathsf{pos}(H')\big) = 0 \quad \forall\, |A|,$$

hence every position-based test (entropy, Kolmogorov–Smirnov) has distinguishing advantage 0 *against Sybil density.*

Proof. $\mathsf{h}(\cdot)$ uniform on R for every key, honest or adversarial; a union of i.i.d. uniforms is distribution-invariant in its partition. □

Placement tests detect biased sampling; the threat is cheap identity. Validation must be cryptographic and economic, and a global random seed is a bootstrap circularity (a randomness beacon presupposes the committee being selected). Both are removed by sortition [7, 8].

Definition 10 (Beacon)**.**

$$\begin{aligned} G_0 &= S \quad \textit{(genesis DKG)},\\ G_k &= \mathsf{vset}(\Sigma_k),\\ \mathsf{TSig}_G &: \ \theta\textit{-of-}|G|,\ \text{unique } \textit{[9]}:\\ &\quad\ |\{\sigma : \mathsf{TVrfy}(\mathsf{gpk}, k, \sigma)\}| = 1 \quad \forall k,\\ B_k &= \mathsf{h}\big(\mathsf{TSig}_{G_{k-1}}(k)\big),\\ \mathsf{gpk} &\in \Sigma \quad \textit{(invariant under } \mathsf{reshare}\textit{)}. \end{aligned}$$

The group is inductive, which breaks the bootstrap circularity in both phases: the already-seated group G_{k-1} *signs the beacon that seats epoch* k*; proactive resharing hands the same* gpk *to each new* vset*, so verification never changes. Remark: all* B_k *are determined at key generation; unpredictability holds only below* θ *shares (as in drand-style beacons) — a* θ*-quorum can precompute every future beacon, which Definition 9 already assumes it must not form adversarially.*

Proposition 6 (Beacon unbiasability)**.**

$$B_k = \mathsf{fn}(\mathsf{gpk}, k) \ \wedge\ \mathsf{predict}(B_k) \Rightarrow \theta \textit{ shares},$$

i.e. no participant choice influences B_k*. A header-hash beacon* $\mathsf{h}(\mathsf{fin}(\Sigma_k))$ *is excluded: proposers grind* B_k *through content selection.*

Proof. Uniqueness leaves a single valid σ per k: the signing protocol has no free variable to grind. Unpredictability below θ shares is the threshold-signature security game. □

Algorithm 1 Trust-weighted sortition (node v, epoch k, role r)

1: $B_k \leftarrow \mathsf{h}(\mathsf{TSig}_{G_{k-1}}(k))$ ▷ Definition 10
2: $(y, \pi) \leftarrow \mathsf{VRF}_{\mathsf{sk}_v}(B_k \| r)$ ▷ sk_v = the DID key
3: $\mathsf{seats}_v \leftarrow \mathrm{InvCDF}_{\mathrm{Bin}(\hat{t}_k(v),\, \tau/\hat{T}_k)}\big(y/2^{|y|}\big)$
4: v holds seats_v seats for r; publishes π

Weight is atomized: node v's fixed-point weight $\hat{t}_k(v)$ (Definition 16) is $\hat{t}_k(v)$ unit atoms, $\hat{T}_k = \sum_v \hat{t}_k(v)$; each atom is selected independently with probability $\tau/\hat{T}_k$, realized per node through the inverse binomial CDF on the VRF output [7]. Atomization removes both hidden hypotheses

of naive indicator sortition: expected seats are exactly proportional to weight with no per-node cap ($\mathbb{E}[\mathsf{seats}_v] = \tau\,\hat{t}_k(v)/\hat{T}_k$, whales simply hold several seats), and normalization by $\hat{T}_k$ makes the fraction well-defined even when total mass is below one (Invariant 1). The DID key doubles as the VRF key: it is committed by v's first appearance in the ledger, hence fixed before any later beacon exists (Proposition 7).

Proposition 7 (Grinding closure)**.**

$$\begin{array}{rcl} \mathsf{sk}_v \textit{ fixed} & \prec & B_k \textit{ exists}, \\ B_k \textit{ unbiasable} & & \textit{(Proposition 6)}, \end{array} \quad \Rightarrow\ \mathsf{grind} = \bot.$$

Proof. Both VRF inputs are committed before either party can condition on the output; unpredictability from Assumption 1 and Proposition 6. □

Proposition 8 (Committee safety)**.** *Atoms are independent indicators, so with $\pi_A = \hat{T}(A)/\hat{T} < \frac{1}{3}$ (Assumption 2, which is fractional), $\mathbb{E}[X] = \tau$ and $\mathbb{E}[X_A] = \tau\,\pi_A$. By Chernoff–Hoeffding over the atom indicators,*

$$\Pr\Big[X_A \geq \tfrac{\tau}{3}\Big] \ \leq\ \exp\Big(-\tau\,\mathrm{D}\big(\tfrac{1}{3}\,\|\,\pi_A\big)\Big),$$

with D *the binary relative entropy: committee dishonesty decays exponentially in committee size. Sortition is the transport of Assumption 2 from weight to seats; no reported quantity exists for a coalition to steer, so the draft's median game is vacuous by construction.*

6 Admission Ledger

Definition 11 (Ledger)**.**

$$\begin{array}{rcl} \Sigma_k & = & \langle \mathsf{rt}(t_k), \mathsf{rt}(V_k), \mathsf{rt}(\mathsf{sl}_k), \mathsf{rt}(\mathsf{bal}_k), \mathsf{gpk}, \mathsf{ver}\rangle, \\ \mathsf{fin}(\Sigma_k) & \equiv & \mathsf{QC}_{2/3}\big(\mathsf{vset}(\Sigma_{k-1})\big) \quad \textit{[10, 11]}, \\ \mathsf{content}_k & = & \{\mathsf{rt}(X_k)\}, \qquad \mathsf{data}(X_k) \in \mathsf{Overlay}. \end{array}$$

Definition 12 (Input block)**.**

$$\begin{array}{rcl} X_k & = & \langle P_k,\, E_k,\, \mathsf{TX}_k,\, \mathsf{fees}_k\rangle, \\ P_k & = & \textit{receipt multiset}, \\ E_k & = & \textit{equivocation proofs}, \\ \mathsf{TX}_k & = & \textit{transfer/bond/unbond ops}, \\ W_k & = & \mathsf{Agg}(P_k):\ \textit{deterministic fold —} \\ & & \textit{dedup } (b,k,n) \textit{ within } P_k\textit{, rows} \\ & & \textit{clipped to } w_{\max} \textit{ in hash order.} \end{array}$$

X_k is assembled by the slot proposer from submissions during $\mathsf{epoch}(k)$*;* Agg *is a pure function of the multiset, so W_k is canonical given X_k. Proposer discretion over* admission *to X_k is exactly the censorship power bounded by Obligation 2.*

Obligation 1 (Minimal trust)**.**

$$\begin{array}{rcl} \forall o \in \mathsf{content}:\ \mathsf{Verify}(o) & \bot & \mathsf{honest}(S), \\ \mathsf{Cap}(\mathsf{quorum}) & = & \{\mathsf{order}, \mathsf{censor}\}, \\ \mathsf{forgeable}(\mathsf{quorum}) \ni o & \Rightarrow & \textit{design defect.} \end{array}$$

Definition 13 (Equivocation proof)**.**

$$e = \langle m_1, \sigma_v(m_1), m_2, \sigma_v(m_2) \rangle,$$

$$\mathsf{slot}(m_1) = \mathsf{slot}(m_2) \ \wedge \ m_1 \neq m_2 \ \Rightarrow \ \mathsf{slash}(v),$$

verification assumption-free; e is a first-class ledger object, submittable by anyone.

Obligation 2 (Force inclusion)**.** *Submissions are acknowledged per slot proposer p:*

$$\mathsf{ack}_p(x) \ \wedge \ \mathsf{proposes}(p, [k, k+\Delta]) \ \wedge \ x \notin X_{[k,k+\Delta]} \ \Rightarrow \ \mathsf{slash}(p),$$

with evidence $\langle \mathsf{ack}_p(x),$ p's signed block$\rangle$ — both signed by p, hence self-certifying and *attributable: the slash lands on the proposer who acknowledged and then withheld, never on a bystander quorum member. Censorship, the residual validator power, is thereby bounded by latency Δ times the number of colluding proposers a submitter must route around.*

Equivocation defeats patience: months of farmed standing forfeit on one contradiction, so $\mathbb{E}[\mathsf{farm}] \downarrow$ with detection probability.

7 Folded State

Browser wasm nodes can neither replay history nor audit a validator signature; the chain must be succinct [12].

Definition 14 (Epoch transition)**.**

$$F(\Sigma_k, X_k) = \Sigma_{k+1}, \qquad \mathsf{rt}(X_k) \text{ public input}, \ X_k \text{ witness},$$

typed against Definition 12: the body consumes the opened block (receipts, proofs, transactions, fees), never bare roots.

Algorithm 2 F — pure, deterministic, per epoch

1: $\mathsf{sl}_{k+1} \leftarrow \mathsf{sl}_k \cup \{\mathsf{verify}(e) : e \in E_k\}$
2: $U \leftarrow V \setminus \mathsf{sl}_{k+1}; \quad t' \leftarrow t_k \restriction_U; \quad s' \leftarrow s \restriction_U; \quad \tilde{C}_k \leftarrow C_k \restriction_{U \times U}$ ▷ Law 3
3: $t_{k+1} \leftarrow \alpha_k \tilde{C}_k^{\mathsf{T}} t' + (1 - \alpha_k)\, s'$ ▷ Eq. (1), Def. 8
4: $\mathsf{bal}' \leftarrow \mathsf{apply}(\mathsf{TX}_k, \mathsf{bal}_k)$ ▷ transfers, bond/unbond; $\mathsf{bal} \geq \mathsf{amt}$
5: $\mathsf{bal}_{k+1} \leftarrow \mathsf{bal}' + \mathsf{issue}(W_k, t_k) - \mathsf{burn}(\mathsf{fees}_k)$
6: $V_{k+1} \leftarrow \mathsf{vset}(\Sigma_{k+1})$ ▷ Obligation 8
7: **return** $\langle \mathsf{rt}(t_{k+1}), \mathsf{rt}(V_{k+1}), \mathsf{rt}(\mathsf{sl}_{k+1}), \mathsf{rt}(\mathsf{bal}_{k+1}), \mathsf{gpk}, \mathsf{ver} \rangle$

$$\mathsf{cost}(F) = O(\mathsf{nnz}(W_k) + |\mathsf{TX}_k|)$$
adds/mults over committed data.

Line 2 restricts vector, matrix (both dimensions), *and* seeds: rows die with $t'(b) = 0$, but columns and s must be cut explicitly or slashed nodes re-accrue mass (Law 3). Line 3 is why the fixpoint is unrolled: one sparse matrix–vector product arithmetizes trivially; an eigenvector solve does not. Line 4 is the transfer semantics of the two-asset economy (Definition 18): apply is sum-preserving, and bond/unbond move balance into and out of Bond with an unbonding delay of Δ_{ub} epochs (slash exposure persists through the delay).

Definition 15 (Folding)**.** *Nova-family IVC [13]:*

$$\begin{array}{rcl} \pi_k & \vdash & \Sigma_0 \xrightarrow{F^k} \Sigma_k, \\ |\pi_k| & = & O(1), \qquad \mathsf{Verify}(\pi_k) = O(1), \\ \mathsf{sync} & = & \mathsf{Verify}(\pi_k) \wedge \mathsf{QC}_{2/3}(\Sigma_k), \\ \mathsf{prove} & \| & \mathsf{consensus} \quad \textit{(asynchronous, trails head).} \end{array}$$

Proposition 9 (Linearity)**.**

$$\mathsf{fin}(\Sigma_k) \textit{ instant (BFT)} \Rightarrow \mathsf{chain} \cong (\Sigma_0, \Sigma_1, \dots) \textit{ linear},$$

hence IVC applies with no re-folding branch; probabilistic-finality chains admit no such reduction.

Proof. Quorum intersection: two finalized blocks at one height require $\geq \frac{1}{3}$ of the finality committee to equivocate (Definition 13) — contradicting Definition 9 in the authority phase, and Proposition 8 with Assumption 2 in the staked phase. □

Obligation 3 (Circuit discipline)**.**

$$\begin{array}{l} \forall \textit{ extension } F' : \\ \qquad F' \textit{ pure} \quad \wedge \quad F' \in \mathsf{CheapArith}(\mathsf{committed}). \end{array}$$

The ledger is an admission ledger, not a contract platform.

Obligation 4 (Verification boundary)**.**

$$\begin{array}{rcl} \textit{in-fold} & : & F \textit{ (state arithmetic over } X_k), \\ \textit{out-of-fold} & : & \mathsf{Vrfy}(\rho),\ \mathsf{VRF}\ \pi,\ \mathsf{TSig}, \\ & & \textit{checked by validators pre-}\mathsf{QC}, \\ \mathsf{QC}(\Sigma' \| \mathsf{rt}(X)) & \Rightarrow & \textit{attests validity}, \\ \mathsf{invalid}\ \rho \in X_k & \Rightarrow & \textit{fraud proof from } X_k \textit{ data} \\ & & \Rightarrow \textit{ quorum slash.} \end{array}$$

Elliptic-curve verifications are not CheapArith *(Obligation 3); the fold proves the arithmetic transition, the quorum attests input validity, and anyone holding* $\mathsf{data}(X_k)$ *can re-check — so forged inputs are not impossible but detectable and slashable, preserving Obligation 1 through accountability rather than circuit cost. In the staked phase the sortition proofs seating* V_{k+1} *live on the same side: verified out-of-fold, consumed by line 6 of Algorithm 2 as committed input.*

Definition 16 (Fixed-point carrier)**.** *Circuits have no reals. With precision* ϕ*:*

$$\begin{array}{rcl} \hat{t} & = & \lfloor t \cdot 2^\phi \rfloor \in \mathbb{Z}_{\geq 0}, \\ \hat{x} \cdot \hat{y} & \mapsto & \lfloor \hat{x}\hat{y}/2^\phi \rfloor, \\ x/y & \mapsto & (q, r) :\ x = qy + r, \\ & & 0 \leq r < y \quad \textit{(witnessed, ranged).} \end{array}$$

Proposition 10 (Rounding soundness)**.** *Floor rounding is one-sided (*$\hat{t}_k \leq t_k 2^\phi$*: weight is never overcounted, so safety bounds survive verbatim), and the accumulated error is damped by the contraction of Proposition 4:*

$$e_{k+1} \leq \bar{\alpha}\, e_k + n\, 2^{-\phi} \ \Rightarrow\ \sup_k e_k \leq \frac{n\, 2^{-\phi}}{1 - \bar{\alpha}},$$

bounded for all time; precision is a parameter, not a drift.

Proof. Each of the n components loses at most $2^{-\phi}$ per epoch to truncation; the prior error enters only through $\bar{\alpha}\, C^{\mathsf{T}}$, which is ℓ_1-nonexpansive scaled by $\bar{\alpha}$; geometric sum. □

Proposition 11 (Carrier boundedness)**.**

$$|\mathsf{carrier}(\hat{t}_k)| \;\le\; 2^{\phi} \qquad \forall k,$$

independent of $|V|$: truncation is garbage collection.

Proof. Invariant 1 in fixed point gives $\sum_v \hat{t}_k(v) \le 2^{\phi}$ atoms; every carried v holds $\hat{t}_k(v) \ge 1$ atom, and a component truncated to 0 leaves the carrier (its Merkle leaf is pruned). Without truncation the carrier grows without bound — geometric decay never reaches zero — so state boundedness is a free consequence of Definition 16, not an extra mechanism. □

Obligation 5 (Upgrade versioning)**.**

$$\begin{aligned} F \mapsto F' \;&\Rightarrow\; \mathsf{vk} \mapsto \mathsf{vk}', \\ \mathsf{ver} \;&\in\; \Sigma, \\ \mathsf{bind}(\mathsf{vk}, \mathsf{vk}') \;&\textit{ at }\; \textit{committed epoch}; \end{aligned}$$

shipped at genesis, not retrofitted.

Folding provides validity only: $\mathsf{canonicity} \in \mathsf{consensus}$, $\mathsf{availability} \in \mathsf{overlay}$.

Definition 17 (Commitment granularity)**.**

$$\begin{aligned} \Gamma \;&\in\; \{\mathsf{full}, \mathsf{agg}, \mathsf{blind}\}, \\ \mathsf{leak}(\mathsf{full}) \;&=\; \{(b, a, W[b, a])\} \quad \textit{(the traffic graph)}, \\ \mathsf{leak}(\mathsf{agg}) \;&=\; \{(v,\ \deg^{\pm}(v))\}, \\ \mathsf{leak}(\mathsf{blind}) \;&=\; \varnothing, \\ \Gamma \neq \mathsf{full} \;&\Rightarrow\; F \textit{ consumes edge data as private} \\ &\qquad\quad \textit{witness (blind: ZK openings)}, \\ \mathsf{replay}(\Gamma) \;&=\; \top \iff \Gamma = \mathsf{full}. \end{aligned}$$

Γ *trades public replayability against surveillance of the service graph; the choice is a standing design decision, and* $\Gamma = \mathsf{blind}$ *prices its privacy in circuit cost (Obligation 3).*

8 State Relation

The ledger state machine in TLA form [14], the model-checking surface for finite instances [15]:

$$\begin{aligned} \mathsf{Spec} \;&\triangleq\; \mathsf{Init} \wedge \Box[\mathsf{Next}]_{\Sigma} \wedge \mathrm{WF}_{\Sigma}(\mathsf{Next}), \\ \mathsf{Init} \;&\triangleq\; \Sigma = \langle \mathsf{rt}(s), \mathsf{rt}(S), \varnothing, \mathsf{rt}(\mathbf{0}), \mathsf{gpk}_0, \mathsf{ver}_0 \rangle, \\ \mathsf{Next} \;&\triangleq\; \exists\, X :\; \mathsf{QC}_{2/3}\big(\Sigma' \| \mathsf{rt}(X)\big) \;\wedge\; \Sigma' = F(\Sigma, X), \end{aligned}$$

with gpk_0 from the genesis DKG (Definition 9).

Invariant 2 (Slash monotone)**.**

$$\mathsf{sl} \subseteq \mathsf{sl}', \qquad v \in \mathsf{sl} \Rightarrow t(v) = 0.$$

Proof. Lines 1–3 of Algorithm 2: sl only grows by union, and the update runs entirely over $U = V \setminus \mathsf{sl}_{k+1}$ — vector t', both dimensions of $\tilde{C}_k$, and seeds s' are restricted, so no term of line 3 can assign mass to a slashed index. (Restricting the vector alone would not suffice: an unrestricted column of C_k, or a fixed $s_v > 0$, re-grants mass one epoch later — hence Law 3 demands all three cuts.) □

Invariant 3 (Version monotone)**.**

$$\mathsf{ver}' \geq \mathsf{ver},$$

by Obligation 5: vk *rebinding occurs only at committed epoch boundaries, forward.*

Invariant 4 (Unique chain)**.**

$$\mathsf{fin}(\Sigma_k) \wedge \mathsf{fin}(\Sigma'_k) \;\Rightarrow\; \Sigma_k = \Sigma'_k,$$

by Proposition 9 (quorum intersection under Assumption 2).

Proposition 12 (Progress)**.** *Under partial synchrony (after global stabilization time) with a live honest quorum — $\theta|S|$ members in the authority phase (Definition 9), honest committee majority via Proposition 8 in the staked phase —*

$$\Box\Diamond\, \mathsf{Next}\text{-}\textit{enabled} \;\wedge\; \mathrm{WF}_{\Sigma}(\mathsf{Next}) \;\Rightarrow\; \forall k :\; \Diamond\, \mathsf{fin}(\Sigma_k).$$

Proof. W may be empty, so Next is enabled whenever a quorum is live; BFT view-change liveness [10] delivers $\mathsf{QC}_{2/3}$ after stabilization; weak fairness converts enabledness into occurrence. □

Obligation 6 (Checkable instances)**.** *Every implementation change to F ships with a finite-instance model ($|V| \leq n_0$, bounded epochs) checking Invariants 1, 2–4 before merge.*

9 Economics

Definition 18 (Two assets)**.**

$$\begin{aligned} \mathsf{rank} \;&:\; \textit{soulbound (Def. 7)},\\ &\quad\; \textit{gates admission/sortition},\\ \mathsf{reward} \;&:\; \textit{transferable via } \mathsf{TX} \textit{ (Alg. 2, l.4)},\\ \mathsf{issue}_k(v) \;&\propto\; \big(W_k^{\mathsf{T}} t_k\big)(v). \end{aligned}$$

Proposition 13 (Countersigning game)**.** *For a service-consuming node b:*

$$\begin{aligned} \mathsf{cost}(\mathsf{sign}) &= 0 \quad \textit{(outflow spends } b\textit{'s row,}\\ &\qquad\qquad \textit{never } t(b)\textit{)},\\ u_b(\mathsf{withhold}) &= \textit{choked: service needs receipts},\\ u_b(\mathsf{sign}) &= \textit{continued service}, \end{aligned}$$

so truthful countersigning is weakly dominant under link-layer tit-for-tat (the eDonkey/BitTorrent heritage [16,17]). Selling receipts is not free-riding but attack-edge formation: the seller's flow enters g of Proposition 2, is volume-capped by $w_{\max}$, and is priced by Proposition 3.

Proposition 14 (Payable rank defeats cost anchoring)**.** *Let rank be transferable at price p. Then*

$$\begin{aligned} \mathsf{cost}_{\mathsf{Adv}}(m) &= \min\big(\mathsf{farm}(m),\; p \cdot m\big),\\ u_{\mathsf{exit}}(\mathsf{hold}) = 0 \;\wedge\; p > 0 &\;\Rightarrow\; \textit{exiting nodes sell},\\ \textit{supply} > 0 &\;\Rightarrow\; p \leq \inf_v \mathsf{farm}_v(m)/m, \end{aligned}$$

so acquisition cost decouples from behavior. Non-transferability removes the second branch of the min*, restoring* $\mathsf{farm}(m) = \textit{service} + \textit{time} + \textit{slash risk}$ *as the sole path.* □

Invariant 5 (Balance conservation)**.**

$$\mathbf{1}^{\mathsf{T}}\mathsf{bal}_{k+1} = \mathbf{1}^{\mathsf{T}}\mathsf{bal}_k + \mathsf{issue}_k - \mathsf{burn}_k,$$

by lines 4–5 of Algorithm 2: $\mathsf{apply}(\mathsf{TX}_k, \cdot)$ *is sum-preserving (transfers permute balance, bond/unbond move it between* bal *and* Bond *within the same total), so supply changes only through published issuance and burn.*

Definition 19 (Fee loop)**.**

$$\begin{aligned} \mathsf{Sinks} &= \{\mathsf{store}_{>\rho},\ \mathsf{QoS},\ \mathsf{namespace}\}, \\ \mathsf{fees} &\to \mathsf{burn} \cup \mathsf{issue\ pool}, \\ \mathsf{anchor}_{\mathsf{PoS}} &\leq f(\mathsf{demand}(\mathsf{Sinks})). \end{aligned}$$

Obligation 7 (Security-budget crossover)**.**

$$\mathsf{activate}(\mathsf{PoS}) \iff \mathsf{Bond} \geq \beta \cdot \widehat{\mathsf{payoff}}(\mathsf{attack}), \quad \beta > 1,$$

conditioned, never scheduled; pre-crossover, PoA finality overlays PoS production, weighted down by $D(\mathsf{vol}_k)$ *(Definition 8).*

Obligation 8 (Validator-set abstraction)**.**

$$\begin{aligned} \mathsf{vset} &: \Sigma \to 2^V, \\ \mathsf{vset}_{\mathsf{PoA}} &= \mathsf{const}\ S, \\ \mathsf{vset}_{\mathsf{PoS}} &= \mathsf{sortition}(\mathsf{Bond}) \\ &\quad \textit{(seat proofs out-of-fold, Obl. 4)}; \end{aligned}$$

the transition changes one pure function, not the engine.

Constraint 1 (Rejected anchors)**.**

$$\begin{aligned} \mathsf{PoW} &: \mathsf{cost}(\textit{51\%}) = \mathsf{rent}(\mathsf{hash}) \cdot O(\textit{hours}) \ \Rightarrow\ \bot, \\ \mathsf{PoT} &: W_{\mathsf{synth}}[b, a],\ a, b \in \mathsf{Adv} \not\perp W_{\mathsf{real}} \\ &\quad \Rightarrow\ \textit{bandwidth burned},\ \Delta T(\mathsf{Adv}) \approx 0 \ \Rightarrow\ \bot. \end{aligned}$$

Receipted real service with trust weighting is proof-of-traffic minus the synthetic load.

10 Security Analysis

Table 1: Threat matrix

Attack	**Bound**	**Residual**
Sybil flood	Prop. 2	$\alpha g/(1-\alpha)$
Self-dealing	Prop. 1 + signer-trust weight; cap (Def. 4)	zero-trust circulation
Patient farming	Laws 1–3; total slash (Def. 13)	undetected deviation
Whitewashing	fresh DID $\Rightarrow t = 0$; slow earn, instant loss	re-entry at zero
Grind/eclipse	Prop. 7	—
Censorship	Obl. 2	latency Δ
Seed compromise	threshold S; revocation; Def. 8	pre-dilution window
Rank market	Prop. 14	out-of-band key sale

$$\begin{aligned} \mathsf{sale}(\mathsf{sk}_v) &\Rightarrow \text{buyer inherits slash exposure,} \\ \mathsf{PoA} &= \text{trust root until Obl. 7.} \end{aligned}$$

Table 2: Protocol parameters

Sym.	Role	Constraint
α_k	damping / seed weight	$\bar{\alpha} = \sup_k \alpha_k < 1$; Def. 8
$w_{\max}$	receipt issuance cap	bounds per-identity sale volume
τ	expected committee size	error $e^{-\tau \mathrm{D}(1/3 \| T(A))}$, Prop. 8
θ	authority threshold	$\geq 2/3$; Defs. 9, 10
Δ	inclusion timeout	censorship latency, Obl. 2
T_{ep}	epoch timer	enables Next, Def. 2
Δ_{ub}	unbonding delay	slash exposure persists, Def. 14
μ	service metering	published per kind, Def. 4
ϕ	fixed-point precision	error $\leq n2^{-\phi}/(1-\bar{\alpha})$, Prop. 10
D	dilution curve	non-increasing, published, Def. 8
β	crossover margin	> 1, Obl. 7

11 Related Work

Local scoring descends from eDonkey queues [16] and BitTorrent choking [17]; propagation from EigenTrust and personalized PageRank [5, 6], here unrolled along epochs over signed evidence; the attack-edge bound pattern from SybilGuard/SybilLimit/SybilRank [18–20], instantiated over a service graph. Brahms [21] addresses adversarial sampling that the draft's tests could not (Proposition 5); DRanking sidesteps via Algorand-style sortition [7, 8] weighted by trust. S/Kademlia [22] prices identifier creation (complementary one-time cost). Finality follows PBFT lineage [10, 11]; succinctness follows Mina [12] via Nova folding [13]; impossibility framing is Douceur's [1]; the external-cost anchor observation is Nakamoto's [23].

12 Conclusion

$$\mathsf{safe} \iff \mathsf{cost}\big(T(\mathsf{Adv}) \geq \tfrac{1}{3}\big) > \widehat{\mathsf{payoff}}(\mathsf{attack}),$$

and every mechanism above — receipts, the trust laws, sortition, the ledger, folding, the two-asset economy — is a term on the left-hand side.

References

[1] J. R. Douceur, "The sybil attack," in *Peer-to-Peer Systems, First International Workshop (IPTPS 2002)*, ser. Lecture Notes in Computer Science, vol. 2429. Springer, 2002, pp. 251–260.

[2] R. J. Kung, "Rings: An algebraic structured peer-to-peer network for decentralized identity and resource ownership," Rings Network 1.0 Whitepaper, 2026, https://rings.rs/papers/rings/.

[3] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," in *Proceedings of the 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*. ACM, 2001, pp. 149–160.

[4] P. Zave, "Reasoning about identifier spaces: How to make Chord correct," *IEEE Transactions on Software Engineering*, vol. 43, no. 12, pp. 1144–1156, 2017.

[5] L. Page, S. Brin, R. Motwani, and T. Winograd, "The PageRank citation ranking: Bringing order to the web," Stanford InfoLab, Tech. Rep. 1999-66, 1999, http://ilpubs.stanford.edu:8090/422/.

[6] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The EigenTrust algorithm for reputation management in P2P networks," in *Proceedings of the 12th International Conference on World Wide Web (WWW 2003)*. ACM, 2003, pp. 640–651.

[7] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling byzantine agreements for cryptocurrencies," in *Proceedings of the 26th Symposium on Operating Systems Principles (SOSP 2017)*. ACM, 2017, pp. 51–68.

[8] S. Micali, M. O. Rabin, and S. P. Vadhan, "Verifiable random functions," in *40th Annual Symposium on Foundations of Computer Science (FOCS 1999)*. IEEE, 1999, pp. 120–130.

[9] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," *Journal of Cryptology*, vol. 17, no. 4, pp. 297–319, 2004.

[10] M. Castro and B. Liskov, "Practical byzantine fault tolerance," in *Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI 1999)*. USENIX Association, 1999, pp. 173–186, https://www.usenix.org/conference/osdi-99/practical-byzantine-fault-tolerance.

[11] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382–401, 1982.

[12] J. Bonneau, I. Meckler, V. Rao, and E. Shapiro, "Mina: Decentralized cryptocurrency at scale," Whitepaper, 2020, https://minaprotocol.com/wp-content/uploads/technicalWhitepaper.pdf.

[13] A. Kothapalli, S. Setty, and I. Tzialla, "Nova: Recursive zero-knowledge arguments from folding schemes," in *Advances in Cryptology – CRYPTO 2022*, ser. Lecture Notes in Computer Science, vol. 13510. Springer, 2022, pp. 359–388.

[14] L. Lamport, *Specifying Systems: The TLA+ Language and Tools for Hardware and Software Engineers*. Addison-Wesley, 2002.

[15] J. Nadal, "Stateright: Model checking for implementing distributed systems," https://www.stateright.rs/, accessed: September 1, 2026.

[16] Y. Kulbak and D. Bickson, "The eMule protocol specification," School of Computer Science and Engineering, The Hebrew University of Jerusalem, Tech. Rep. TR-2005-03, 2005.

[17] B. Cohen, "Incentives build robustness in BitTorrent," Workshop on Economics of Peer-to-Peer Systems, 2003, https://www.bittorrent.org/bittorrentecon.pdf.

[18] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "SybilGuard: Defending against sybil attacks via social networks," in *Proceedings of the 2006 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM 2006)*. ACM, 2006, pp. 267–278.

[19] H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, "SybilLimit: A near-optimal social network defense against sybil attacks," in *2008 IEEE Symposium on Security and Privacy*. IEEE, 2008, pp. 3–17.

[20] Q. Cao, M. Sirivianos, X. Yang, and T. Pregueiro, "Aiding the detection of fake accounts in large scale social online services," in *9th USENIX Symposium on Networked Systems Design and Implementation (NSDI 2012)*. USENIX Association, 2012, pp. 197–210, https://www.usenix.org/conference/nsdi12/technical-sessions/presentation/cao.

[21] E. Bortnikov, M. Gurevich, I. Keidar, G. Kliot, and A. Shraer, "Brahms: Byzantine resilient random membership sampling," *Computer Networks*, vol. 53, no. 13, pp. 2340–2359, 2009.

[22] I. Baumgart and S. Mies, "S/Kademlia: A practicable approach towards secure key-based routing," in *2007 International Conference on Parallel and Distributed Systems*. IEEE, 2007, pp. 1–8.

[23] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Whitepaper, 2008, https://bitcoin.org/bitcoin.pdf.