The ADIC-DAG Yellow Paper

Formalization, Conjectures, and Partial Results

Samuel Reid

August 20 2025

MSC 2020: 68M12, 68M14, 05C65, 55N31, 11S80, 94A60, 91A43

Abstract

This *Yellow Paper* formalizes the ADIC-DAG protocol as introduced in the White Paper and extends it with precise state-machine semantics, admissibility invariants, and mathematically stated conjectures together with partial results and proof sketches. The core ideas—a p-adic ultrametric on message features, higher-dimensional Tangle attachments (each message approves $d+1$ parents), and dual finality tests via k-core coverage and persistent homology—are specified in a way intended to be machine-checkable and implementable. We also present a reference generative model, security assumptions, parameter phase diagrams near $(p, d) = (3, 3)$, and an open-problem bank with acceptance criteria for decentralized research and bounties.

Contents

1 Introduction and Design Goals

ADIC-DAG is a feeless, reputation-weighted distributed ledger where each message attaches to $d+1$ parents across distinct p-adic neighborhoods (axes), enforcing multi-axis diversity at the moment of attachment. Finality is certified by two independent tests: (F1) a k-core coverage criterion with axis-diversity and reputation thresholds; and (F2) stabilization of weighted persistent homology in the future cone. The ADIC token funds utility (storage, PoUW bounties, governance) but *not* consensus security; consensus weight derives from refundable deposits and a non-transferable reputation (ADIC-Rep).

Notation. Fix a prime p and a dimension $d \in \{2, 3, \ldots\}$. Each message x carries features $\Phi(x) = (\varphi_1(x), \ldots, \varphi_d(x)) \in \mathbb{Q}_p^d$, a public key P_x, a reputation $R(P_x) \geq 0$, and an approval set $A(x) = \{a_0, \ldots, a_d\}$ respecting acyclicity. Let $\rho = (\rho_1, \ldots, \rho_d) \in \mathbb{Z}_{\geq 0}^d$ be axis radii and $q \in \{2, \ldots, d+1\}$ a diversity threshold.

2 System Model and State Machine

2.1 The simplicial DAG and future cones

Definition 2.1 (Simplicial hypergraph)**.** The ledger state at any time is a directed acyclic simplicial hypergraph $T_d = (V, \Sigma_d)$ where every $x \in V$ adds a simplex $\{x, a_0, \ldots, a_d\} \in \Sigma_d$ with directed approvals $x \to a_i$, and with no directed cycles. The *future cone* of x is the set of y that (transitively) approve x.

Definition 2.2 (Admissibility and diversity)**.** Given ρ, q, a candidate approval set $A(x) = \{a_0, \dots, a_d\}$ is *admissible* if, for each axis $j \in \{1, \dots, d\}$,

(C1) $\mathrm{v}_p(\varphi_j(x) - \varphi_j(a_i)) \geq \rho_j$ for all i;

(C2) the multiset of p-adic balls $\{B^{(p)}(\varphi_j(a_i), \rho_j)\}_{i=0}^{d}$ contains at least q *distinct* balls;

(C3) $\sum_{i=0}^{d} R(a_i) \geq R_{\min}$ and $\min_i R(a_i) \geq r_{\min}$.

2.2 Node state machine

Each node maintains:

- a local view of tips $T \subset V$ (vertices with no incoming approvals),
- per-axis vector clocks to ensure acyclicity on arrival,
- an escrow ledger of deposits D and refunds,
- an estimator for finality (F1)/(F2) with parameters $(k, q, R^*, D^*, \Delta, \varepsilon)$.

The transition function ValidateAndAttach checks signature, format, acyclicity, admissibility, escrows D, and appends the simplex. Periodic Finalize runs (F1) and/or (F2); on success it refunds D and updates ADIC-Rep.

3 Tip Selection by Multi-Axis Random Walk (MRW)

Definition 3.1 (MRW kernel)**.** Let $\mathrm{proxp}(x, y) := \prod_{j=1}^{d} \big(1 + p^{\rho_j - \mathrm{v}_p(\varphi_j(x) - \varphi_j(y))}\big)^{-1}$ and $\mathrm{trust}(y) := R(y)^{\alpha}/(1 + \mathrm{age}(y))^{\beta}$. With $\mu, \lambda > 0$ and conflict penalty $\mathrm{conflict}(y) \in \{0, 1, \dots\}$, define

$$\Pr(t \to y) \;\propto\; \exp\!\big(\lambda\, \mathrm{proxp}(x, y)\, \mathrm{trust}(y) - \mu\, \mathrm{conflict}(y)\big).$$

Run MRW independently per axis, intersect or diversity-merge candidates, then sample a distinct d+1-tuple satisfying (C1)–(C3).

```
# Tip selection (reference)
C = {}                   # candidates per axis
for j in {1..d}:
  C_j = MRW_on_axis(j, x, T, lambda, mu)
C = IntersectionOrDiverseMerge(C_1,...,C_d)
Sample A subset C with |A|=d+1:
  if Admissible(x, A): return A
fallback: widen radii or increase MRW horizon
```

Remark 3.2 (No-starvation desideratum)*.* We seek parameter regimes $(\lambda, \mu, \alpha, \beta)$ under which honest tips below a given reputation percentile receive a non-vanishing visitation frequency. See Conjecture 9.4.

4 Conflict Energy and Drift

For a conflict set C (e.g. mutually exclusive UTXO spends), define

$$\mathrm{supp}(z; C) = \sum_{y \text{ descends to } z} \frac{R(y)}{1 + \mathrm{depth}(y)}, \qquad E = \sum_{C} \sum_{z \in C} \mathrm{sgn}(z)\, \mathrm{supp}(z; C).$$

Conjecture 4.1 (Negative drift of conflict energy)**.** *Under MRW and admissibility (C1)–(C3), there exist $c, \delta > 0$ (depending on $\lambda, \mu, \rho, q, \alpha, \beta$) such that*

$$\mathbb{E}[E(t+1) - E(t) \mid \mathcal{F}_t] \;\leq\; -c\, \mathbf{1}_{\{E(t) > \delta\}},$$

hence conflicts resolve to a unique winner with finite expected time and subexponential tails.

Attempted proof. Couple MRW to a time-changed birth–death process on support differences; use admissibility to bound the probability that newly arriving mass can concentrate on a losing branch across q distinct balls per axis. A supermartingale argument with optional stopping yields the claimed drift. Completing the proof requires (i) explicit mixing bounds for MRW (Sec. 9.2) and (ii) a uniform anti-concentration bound across axes. $\triangleright$

5 Finality: k-Core and Persistent Homology

Definition 5.1 (Finality tests)**.** A node x is *final* if either:

(F1) (***k*-core**) The future cone of x contains a k-core with at least q distinct p-adic balls per axis, total reputation $\geq R^*$, and minimum depth $\geq D^*$.

(F2) (**Homology**) In the induced weighted simplicial complex, H_d stabilizes over a window of Δ rounds and the bottleneck distance on H_{d-1} falls below ε.

Conjecture 5.2 (Implication gap)**.** *There exist thresholds $(k, q, R^*, D^*, \Delta, \varepsilon)$ such that, for the ADIC generative model, (F1) implies (F2) with probability $1 - \delta$. Quantify minimal such tuples and δ.*

Proof sketch. Model the future cone as a d-simplicial percolation process constrained by (C1)–(C3). A dense k-core distributed across q balls per axis forces stabilization of higher-dimensional cycles: high-weight d-simplices fill d-holes while keeping $(d-1)$-noise below the ε threshold, yielding (F2). A quantitative proof needs explicit isoperimetric inequalities on the product ultrametric and stability of persistent diagrams under weighted additions. $\triangle$

6 Economics and Reputation

6.1 Feeless base and refundable deposits

Every message escrows a deposit D refunded on finality; objective faults (invalid signature, malformed approvals, provable sybil overlap) trigger slashing of D. Fees are not required for liveness or safety.

6.2 ADIC-Rep (reputation)

Definition 6.1 (Reputation update)**.** For public key P,

$$R_{t+1}(P) = \gamma R_t(P) + (1-\gamma)\big(\mathrm{good}(P) - \mathrm{bad}(P)\big),$$

where good credits finalized approvals with diversity/depth weighting and bad penalizes overlap across axes. Only R (not ADIC balances) affects consensus weight.

Conjecture 6.2 (Stability and boundedness)**.** *For appropriate $(\gamma, \eta, \text{caps})$, the reputation dynamics are globally stable and uniformly bounded against any finite-budget adversary.*

Attempted proof. Construct a Lyapunov function $L = \sum_P w_P R(P)$ with weights inversely proportional to axis-overlap rates. Show $\mathbb{E}[L_{t+1} - L_t] \le -\xi \sum_P R(P)$ outside a compact set. The main gap is a tight bound on overlap estimators under adaptive adversaries. ▷

7 Parameters and Safe Operating Regions

7.1 v1 defaults

We adopt $(p, d) = (3, 3)$, $\rho = (2, 2, 1)$, $q = 3$, $k = 20$, $D^* = 12$, window $\Delta = 5$, reputation exponents $(\alpha, \beta) = (1, 1)$, and deposit $D = 0.1$ ADIC as a reference point for analysis and benchmarks.

7.2 Phase diagram (conceptual)

We consider the region in $(p, d, \rho, q, k, D^*, \Delta, \lambda, \mu, \alpha, \beta)$ space separating liveness (non-empty admissible tip set, bounded confirmation latency) from finality failure (persistent topological noise or absence of diversified k-cores). A formal map is left as Conjecture **??**.

8 Security Model

Adversarial goals include sybil concentration (violating (C2)), censorship (starving honest tips), and double-spend (sustaining conflicting support). Defenses: refundable deposits, soul-bound reputation, MRW across axes, diversity thresholds, and dual finality with topological stabilization.

9 Open Problems and Partial Results

Below we formalize key problems as conjectures/theorems. Each has a "counts-as-solved" target for decentralized bounties.

9.1 Ultrametric embeddings and diversity

Conjecture 9.1 (Low-distortion encoders)**.** *Construct $\Phi : \mathcal{X} \to \mathbb{Q}_p^d$ for discrete features with distortion bounded by a function of (p, d) while preserving radii constraints in (C1)–(C2).*

Attempted proof. Use base-p digit interleaving and Hensel lifting for hierarchical buckets; prove that the p-adic distance between encodings lower-bounds axis separation after coarse-graining. Gaps: optimal constants and adversarial worst cases. ▷

Conjecture 9.2 (Minimal diversity threshold)**.** *For fixed (p, d, ρ), there exists $q_{\min}$ such that $q \ge q_{\min}$ makes long-term axis capture by any bounded-budget coalition exponentially unlikely.*

Proof sketch. Model approvals as occupancy in product p-adic trees; apply multi-type branching bounds and Chernoff-style tail inequalities across axes. △

9.2 MRW mixing and fairness

Conjecture 9.3 (MRW mixing time)**.** *The MRW mixes to a stationary measure in* $\tilde{O}(\mathrm{poly}(d)/\mathrm{gap})$ *steps uniformly over time (with mild degree/age regularity).*

Conjecture 9.4 (Fairness under heterogeneous reputations)**.** *Under suitable* $(\lambda, \mu, \alpha, \beta)$*, honest tips below any fixed reputation percentile receive a minimum visitation frequency* $\geq \theta > 0$*.*

Attempted proof. Bound conductance of the MRW kernel by decoupling axis-wise transitions; apply path-congestion techniques to obtain a spectral-gap lower bound depending on (ρ, q) and degree regularity. ▷

9.3 Percolation, cores, and homology

Conjecture 9.5 (Core threshold with diversity)**.** *In a random ADIC-like directed d-simplicial hypergraph with constraints (C1)–(C3), the emergence of a k-core that is q-diverse per axis exhibits a sharp threshold in average attachment rate.*

Conjecture 9.6 (F1 vs. F2 separation)**.** *There exist parameter families where (F1) holds but (F2) fails (or vice versa), with explicit topological obstructions.*

Attempted proof. Construct gadgets of d-simplices that sustain a k-core yet maintain transient $(d-1)$ cycles above the ε bottleneck until additional cross-axis attachments occur. ▷

9.4 Reputation dynamics

Conjecture 9.7 (Collusion resistance)**.** *There exist* $(\gamma, \eta, caps)$ *such that no coalition can raise average reputation above honest baselines without violating (C2).*

9.5 Mechanism design

Conjecture 9.8 (Minimal refundable deposit)**.** *There is a threshold $D^\dagger$ (in units tied to workload) above which spam/overlap attacks are suboptimal for any attacker with bounded variance in issuance rate.*

Conjecture 9.9 (Potential-game formulation)**.** *The attach/approve game admits a potential whose local maxima coincide with equilibria maximizing diversity and liveness.*

9.6 Complexity bounds

Conjecture 9.10 (Dynamic finality complexity)**.** *The online decision "is x final under (F1)/(F2)?" is fixed-parameter tractable in D^* and local degree, or else admits conditional lower bounds (e.g. SETH) for general streams.*

Conjecture 9.11 (Near-log update for homology)**.** *There exists a dynamic algorithm that maintains H_d and H_{d-1} with amortized $O(\log^c m)$ updates for ADIC-style streams, or else an $\Omega(m^\epsilon)$ lower bound holds.*

10 Reference Specification (Condensed)

10.1 Admissibility score

For $A = \{a_0, \ldots, a_d\}$ define

$$S(x; A) = \sum_{j=1}^{d} \min_{a \in A} p^{-\max\{0, \rho_j - \mathrm{v}_p(\varphi_j(x) - \varphi_j(a))\}}.$$

Require $S(x; A) \geq d$ and (C2)–(C3).

10.2 Validation and finality

```
Validate(x):
  check signature, format, per-axis acyclicity
  assert Admissible(x, A(x))
  escrow deposit D
Finalize():
  test F1 and/or F2 on candidates
  refund D on finality; update ADIC-Rep; slash faults
```

11 Generative Model for Analysis

We consider a time-indexed process where honest arrivals follow a renewal process with bounded inter-arrival variance, features $\Phi(x)$ are drawn from axis-specific distributions with Lipschitz densities in the p-adic topology, and adversaries can adaptively choose features and timing subject to deposit costs. This model underlies Conjectures 4.1, 5.2, 9.3.

12 Toward Machine-Checkable Proofs

We recommend formalizing *(i)* admissibility invariants, *(ii)* MRW kernel properties, and *(iii)* finality criteria as executable properties in a proof assistant (e.g. Coq/Lean). The p-adic arithmetic, ultrametric balls, and simplicial complexes are standard libraries or straightforward to encode.

13 Implementation Roadmap (Aligned to Proof Obligations)

Phase 0 (prototype): message format, encoders, MRW, admissibility, k-core, deposits/refunds, explorer.
Phase 1 (beta): streaming homology library, ADIC-Rep SBT, axis-aware gossip, anti-entropy checkpoints.
Phase 2 (mainnet-candidate): PoUW hooks, storage markets, governance (quadratic), parameter sweeps, adversarial testing.

14 Genesis (Informative)

The Genesis hyperedge uses $(p, d) = (3, 3)$ with anchors in distinct balls; the manifest (parameters, anchors, multisig) is anchored on multiple L1s for timestamping. *Contribution addresses for legacy L1 coordination:*

BTC
`bc1qnykv3t8fqpar7aguaas3sxtlsqyndxrpa0g7h8`

ETH
`0x7EB0c7ea79D85d2A3Ac45aF6A8CB0F7AC9A125bE`

SOL
`GrUy83AAsibyrcUtpAVA8VgpnQSgyCAb1d8Je8MXNGLJ`.

Contributions fund R&D and infrastructure; no returns are promised or implied.

15 Conclusion

ADIC-DAG formalizes a feeless consensus with multi-axis diversity and dual finality grounded in combinatorics and topology. The conjectures herein chart the path for decentralized mathematical research that will harden guarantees and tune parameters ahead of mainnet.

A Problem Bank (Canonical Statements & Acceptance Criteria)

Each item below includes a crisp target for acceptance.

A. p-Adic Geometry & Axis Encodings

Conjecture A.1 (A1: Low-distortion ultrametric encoders)**.** *Given discrete feature sets, produce $\Phi : \mathcal{X} \to \mathbb{Q}_p^d$ with distortion $\leq f(p, d)$ s.t. (C1)–(C2) hold.* ***Accept if:*** *worst-case or distributional bounds & explicit encoder.*

Conjecture A.2 (A2: Minimal diversity thresholds)**.** *There exists $q_{\min}$ achieving exponentially small capture probability for bounded-budget coalitions.* ***Accept if:*** *non-asymptotic tail bounds vs. q, ρ and budget.*

B. MRW on Ultrametrics

Conjecture A.3 (B1: MRW mixing)**.** *TV mixing in $\tilde{O}(\mathrm{poly}(d)/\mathrm{gap})$.* ***Accept if:*** *rigorous upper bounds; or matching lower bounds.*

Conjecture A.4 (B2: Hitting diverse parents)**.** *Within T^* steps MRW selects $d{+}1$ admissible parents per (C1)–(C3).* ***Accept if:*** *non-trivial upper/lower bounds or sharp asymptotics.*

C. Conflict Energy

Conjecture A.5 (C1: Explicit drift)**.** *Quantify $c(\cdot)$, prove $\mathbb{E}[\tau_{\text{resolve}}] \leq C \log(1 + |\mathit{support}|)$.* ***Accept if:*** *drift & tail bounds.*

D. Finality via k-Core and Homology

Conjecture A.6 (D1: (F1)⇒(F2))**.** *Specify minimal* $(k, q, R^*, D^*, \Delta, \varepsilon)$ *yielding (F2) w.h.p.* ***Accept if:*** *thresholds & failure* δ *proved.*

Conjecture A.7 (D2: Separation)**.** *Families where (F1) holds and (F2) fails (or vice versa).* ***Accept if:*** *explicit constructions & proofs.*

E. Hypergraph Percolation

Conjecture A.8 (E1: Core threshold with diversity)**.** *Sharp threshold for q-diverse k-core.* ***Accept if:*** *threshold or finite-size scaling with bounds.*

F. Reputation Dynamics

Conjecture A.9 (F1: Stability)**.** *Global stability & boundedness for* $(\gamma, \eta, caps)$*.* ***Accept if:*** *Lyapunov proof with explicit bounds.*

G. Deposits and Mechanism Design

Conjecture A.10 (G1: Minimal refundable deposit)**.** *Threshold* $D^\dagger$ *making spam/overlap attacks suboptimal.* ***Accept if:*** *attacker-model proof & sensitivity.*

K. Complexity

Conjecture A.11 (K1: Dynamic finality complexity)**.** *FPT in* D^* *and local degree or conditional hardness.* ***Accept if:*** *formal classification.*

B Reference Pseudocode

```
# Axis-aware gossip (informal):
on_receive(msg x):
  if not verify_signature(x): reject
  if not acyclic_per_axis(x): queue/later
  if not admissible(x): reject
  escrow_deposit(x.P, D)
  attach_simplex(x, A(x))
  for neighbor in peers:
    send_if_useful(neighbor, x)

# Finality loop:
every t_f seconds:
  candidates = select_recent()
  for x in candidates:
    if KCoreFinal(x, k, q, R*, D*): finalize(x); refund(x.P, D)
    else if HomologyFinal(x, Delta, Epsilon): finalize(x); refund(x.P, D)
```