Randomness.net:
A Decentralized, Unbiasable Randomness Beacon
Without Consensus, Tokens, or Trusted Hardware

Draft v0.1 — Summary Specification

Abstract
We propose a decentralized randomness beacon that produces public, unbiasable, verifiable randomness at sub-second intervals without requiring consensus, staking, threshold signatures, trusted hardware, or a native token. The system combines multiparty entropy contributions, deterministic aggregation, verifiable delay functions (VDFs), and periodic anchoring to Bitcoin to create a globally auditable, tamper-evident log of randomness outputs. Access is monetized via LSAT-backed Lightning micropayments. The architecture provides fault tolerance, resistance to grinding and withholding, simplicity of implementation, and horizontal scalability across multiple independent beacon chains.

1. Introduction
Many systems require unbiased randomness. Existing approaches suffer from centralization, biasability, token dependencies, or cryptographic ceremony complexity. We describe a beacon that avoids these issues by eliminating trusted roles. Liveness does not depend on consensus or leaders. Unpredictability arises from multiparty entropy; unbiasability is enforced by VDFs; and global consistency emerges from deterministic validity rules rather than voting.

2. System Model
Three node classes exist: Entropy Providers (EPs), VDF Workers, and Gateways. All participate in a gossip network. The minimal security assumption is that at least one EP is honest per round.

3. Rounds and Timing
Time is divided into fixed rounds. Each round has a contribution window and a VDF evaluation window. Nodes require only round-number agreement, not tight clock synchronization.

4. Entropy Contribution
EPs submit signed entropy messages. Nodes accept one contribution per EP per round. Invalid or late contributions are ignored.

5. Deterministic Aggregation
Nodes compute XOR of valid entropy contributions and build a Merkle root over them. These values form the canonical VDF input.

6. Unique Canonical Input
Although nodes may temporarily observe different subsets due to latency, validity rules ensure exactly one globally valid subset. Invalid aggregates cannot match the final VDF result.

7. Verifiable Delay Function
A sequential VDF produces an output and proof. Computing the VDF takes fixed real time; verification is fast. Wrong inputs fail verification.

8. Round Result

A round record includes round number, Merkle root, entropy aggregate, VDF output, proof, and previous round hash. Verification rules guarantee uniqueness.

9. Fault Tolerance

EPs and VDF workers may fail without affecting correctness. Gateways are stateless. Missed contributions do not fork the system; invalid VDF results are rejected.

10. Anchoring

Every k rounds, a hash of recent rounds is committed to Bitcoin. Anchoring provides timestamping and long-term tamper resistance.

11. Economic Model

Access is monetized via LSAT and Lightning micropayments. No native token is required. EPs and workers may be compensated in bitcoin.

12. Security Analysis

Unpredictability requires one honest EP. VDFs provide unbiasability. Censorship resistance is achieved through open participation. Invalid aggregates cannot pass verification. Anchoring prevents history rewriting.

13. Comparison to Existing Systems

This design avoids centralization, DKG complexity, oracle trust, and biasability present in other approaches.

14. Horizontal Scalability

Multiple parallel beacons can operate concurrently, enabling higher throughput or domain separation.

15. Conclusion

This beacon achieves decentralization, unbiasability, economic sustainability, and global auditability without consensus or threshold cryptography.