PHOTREK

Reputation & Voting Weight System
Product Requirements Document

1. Executive Summary

The Reputation & Voting Weight System aims to improve the decision-making process in SingularityNET's Deep Funding (DF) governance model by incorporating non-monetary contributions into voting weights. The system introduces a modular microservices-based architecture, allowing flexible reputation score calculations based on diverse forms of participation. It ensures privacy-preserving identity verification, pseudonymous reputation scoring, and expandability for future decentralized identity (DID) and Zero-Knowledge Proof (ZKP) integrations.

This document defines the detailed requirements of the system, covering architecture, microservices, user interface, integration, security, and compliance needs.

2. System Objectives

2.1 Primary Goals

- Enable fairer governance by incorporating contributions (beyond token holdings) into voting weight calculations.
- Support multiple reputation sources through a modular microservices architecture.
- Ensure privacy and security through pseudo-identity mapping and ZKP-ready architecture.
- Integrate with WaLT for decentralized identity (DID) compatibility while maintaining privacy-first principles.
- Allow configurability for different voting scenarios, allowing communities to define reputation models.

2.2 Future Expansion Goals

- Full ZKP integration to enable privacy-preserving on-chain reputation scoring.
- Decentralized Governance Mechanisms (e.g., DAO-driven management).
- AI-powered reputation enhancements, such as fraud detection models.
- Interoperability with broader Web3 ecosystems, enabling cross-platform reputation portability.

3. System Architecture & Design

3.1 High-Level Architecture

The system consists of three core layers:

1. Identity & Authentication Layer

- Wallet Address & DF Profile Mapping: Connect multiple wallets and DF profiles to a single pseudo-identity (pseudo-ID).
- WaLT Integration: Enable compatibility with SingularityNET's Wallet Linking Tool (WaLT).
- Future ZKP Integration: Architect the system for Zero-Knowledge Proof-based identity verification.

2. Reputation Computation Layer

- Microservices-Driven Design: Reputation is computed by independent, configurable microservices.
- Scoring Aggregation Engine: Combines multiple microservice outputs into a final reputation score.
- Role-Based Access Controls:
    - Users: Can view their own reputation data.
    - Admins/Developers: Can oversee scoring models and monitor system behavior.

3. Application & User Interface Layer

- Configurable UI: Users can select microservices, adjust weights, and run calculations.
- Reporting & Analytics: Visualization of historical reputation trends and contributions.
- Export & API Access: Support CSV, JSON, PDF exports and API-based access for external integrations.

4. Functional Requirements

4.1 Must-Have Features

A. Identity & Reputation Mapping

- Wallet & DF Profile Linking:
    - Map wallets + DF profiles to a single pseudo-ID.
    - Ensure one pseudo-ID per human to prevent Sybil attacks.
- Privacy-Preserving ID Handling:
    - Pseudo-ID mappings are hidden from normal users but accessible to admins/developers.
    - Reputation scores are calculated without exposing real identities.

B. Reputation Computation & Weighting

- Configurable Microservices:
    - Allow users to select scoring microservices based on contributions (e.g., engagement, voting history, AGIX holdings, proposal participation, etc.).
    - Enable assigning weights to each microservice's output.
- Standardized APIs for Data Flow:

    - APIs must support secure data exchange between microservices, reputation system, and external tools.
- Error Handling & Fault Isolation:
    - Ensure microservices operate independently, preventing system-wide failures.

C. User Interface & Governance

- User-Friendly UI:
    - Provide dashboard-style interactions for reputation configuration and monitoring.
- Role-Based Permissions:
    - Users: View own scores.
    - Admins: Configure weighting models, microservices, and integrations.
- Reporting & Analytics:
    - Allow users to export reputation data and view trends.

D. Security & Compliance

- Pseudonymization & Anonymization Mechanisms to protect user identity.
- Integration Readiness for Zero-Knowledge Proofs (ZKP) to improve privacy in reputation calculations.
- Compliance with GDPR & CCPA by ensuring data transparency and revocation rights.

5. Roadmap for Future Enhancements

Phase	Milestone	Description
1	**MVP System**	Core **reputation microservices, UI, APIs**
2	**WaLT Integration**	Connect **Wallet Linking Tool** for decentralized identity
3	**ZKP Research**	Define requirements for **Zero-Knowledge Proof privacy**
4	**ZKP Integration**	Implement **ZKP-based identity verification**

6. Knowledge Graph (KG) Enhancements

6.1 Existing KG framework

- The existing KG framework supports data injection, querying, and modification.

- KG is flexible in structure, allowing future integrations with reputation scoring.
- Reference: https://deepfunding.ai/proposal/scalable-metta-knowledge-graphs/

6.2 Potential Enhancements

- Microservice Integration with KG
    - Allow KG to store & process decentralized reputation data.
- Hybrid Reputation Model: KG + Bayesian Networks
    - KG provides structured relationships.
    - Bayesian models offer probabilistic trust scores.
- ZKP-Enhanced Queries
    - Implement privacy-focused query systems for KG reputation insights.

6.3 Research & Next Steps

- Evaluate the feasibility of integrating KG with ZKP privacy models.
- Assess community-driven governance for KG structure modifications.

7. Conclusion

The Reputation & Voting Weight System represents a significant shift in how governance is conducted within SingularityNET’s Deep Funding program. The combination of microservices, privacy-first identity handling, and knowledge graph integrations lays the groundwork for a decentralized, trust-driven governance model.

By designing the system to be ZKP-ready from the start, we ensure that future enhancements such as decentralized identity verification, scalable privacy measures, and AI-assisted reputation modeling can be smoothly integrated as the ecosystem evolves.