MANTECH Publications

Journal of Blockchain Systems and Smart Contracts
Volume 2, Issue 2, May-August 2026
ISSN: 3139-132X (Online)

Reputation-Based Decentralized Governance Using Smart Contracts for Transparent and Manipulation-Resistant DAO Voting

Shivani Bansal[1], Rituraj Rawat[2], Vandana Rajput[3], Abhishek Sharma[4]

ABSTRACT

Decentralized autonomous organizations (DAOs) use blockchain infrastructure and smart contracts to coordinate collective decisions, allocate treasury resources, and modify protocol rules. Yet token-weighted voting may concentrate decision-making power among large holders, while identity-based voting can be vulnerable to Sybil attacks and reputation systems can be manipulated through contribution farming, collusion, or entrenched social hierarchies. This paper reviews relevant DAO governance research and proposes a layered reputation-based voting framework designed to improve transparency while limiting common manipulation pathways. The framework separates reputation evidence from token ownership, uses contribution categories and time-sensitive reputation, constrains individual voting influence, and combines proposal validation, commitment–reveal voting where appropriate, quorum rules, timelocks, audit events, and bounded challenge procedures. It also identifies trade-offs involving privacy, participation costs, accessibility, governance capture, and smart-contract security. This manuscript is a narrative review and design proposal, not a report of a deployed system or an empirical experiment. Accordingly, it does not claim measured performance gains. The proposed architecture should be evaluated through formal threat modelling, adversarial simulations, smart-contract testing, and controlled pilot deployment before use in high-value governance.

KEYWORDS: *Decentralized autonomous organization; DAO; smart contracts; reputation-based voting; Sybil resistance; governance security; blockchain; vote manipulation; transparency.*

Page 70-82 © MANTECH PUBLICATIONS 2026. All Rights Reserved

INTRODUCTION

Decentralized autonomous organizations seek to coordinate participants through shared rules, on-chain assets, proposal processes, and collective voting. Smart contracts can make parts of this process auditable and deterministic, but they do not by themselves guarantee fair representation, meaningful participation, or resistance to strategic behavior. Governance outcomes depend on the voting rule, the distribution of voting resources, the information shown to participants, and the implementation path that follows a vote.

Research has documented the concentration of voting power in prominent DAOs and the challenges of balancing resistance to wealthy domination with resistance to Sybil identities. Quadratic voting, time-commitment mechanisms, delegation, and reputation-weighted approaches address different parts of this problem, but none is universally robust. Reputation can reflect sustained contribution rather than financial stake, yet it can also reward insiders, become difficult to challenge, or be artificially accumulated.

This paper synthesizes relevant literature and proposes a practical framework for reputation-based DAO governance. It emphasizes a key distinction: transparency should make rules, evidence types, proposal states, vote totals, and execution outcomes auditable without automatically exposing every voter's personal identity or private ballot.

PROBLEM STATEMENT

A DAO voting system may be manipulated when voting influence can be purchased, multiplied through pseudonymous identities, accumulated by a small group, or exercised through bribery and coordinated behavior. A purely token-weighted rule risks plutocratic outcomes; a one-address-one-vote rule is vulnerable when address creation is cheap; and a reputation-only system may privilege long-standing members or create incentives to game contribution metrics. The design problem is therefore multi-objective: reduce manipulation while preserving legitimacy, privacy, participation, explainability, and operational reliability.

AIM AND OBJECTIVES

Aim: To develop an evidence-informed conceptual framework for transparent, reputation-based DAO voting implemented through smart contracts.

- To review common DAO voting models and their security and fairness limitations.

Page 70-82 © MANTECH PUBLICATIONS 2026. All Rights Reserved

- To define reputation inputs that can be audited without equating reputation with wealth or popularity.
- To specify a smart-contract workflow for proposal validation, voting, quorum checks, challenges, and execution.
- To identify attack scenarios and layered mitigations for Sybil activity, reputation farming, collusion, and contract vulnerabilities.
- To propose evaluation metrics and a research plan for testing the framework without presenting unmeasured outcomes as established results.

METHODOLOGY

This manuscript uses a focused narrative review of peer-reviewed and scholarly sources on DAO governance, token concentration, reputation-based voting, Sybil resistance, quadratic voting, and governance design. Sources were selected for direct relevance to voting power, manipulation resistance, and implementation constraints. The review is not a registered systematic review; no claim is made that all available studies were identified. The framework is a design synthesis derived from these sources and from general smart-contract security principles.

No original participant dataset, on-chain transaction dataset, deployed-contract audit, or experimental benchmark was supplied for this manuscript. Therefore, the paper reports no invented sample sizes, performance results, statistical tests, or claims of demonstrated superiority.

BACKGROUND AND RELATED WORK

Token-Weighted Governance And Concentration

Token-weighted voting is easy to understand and can align governance rights with economic exposure. However, when token ownership is concentrated, a small set of addresses may hold substantial influence. An empirical analysis of Compound, Uniswap, and ENS governance found voting power concentrated among a small number of addresses, while noting that powerful actors did not frequently overturn outcomes in opposition to the broader community. Concentration is therefore a structural risk indicator, not proof that every vote is captured.

Page 70-82 © MANTECH PUBLICATIONS 2026. All Rights Reserved

Quadratic And Time-Commitment Mechanisms

Quadratic voting increases the marginal cost of accumulating additional votes and can reduce the direct translation of wealth into voting power. However, research has shown that quadratic voting alone may remain vulnerable to collusion. Bond or time-commitment voting introduces a second resource—time locked into a decision—which may raise the cost of Sybil strategies and short-term manipulation under specified assumptions. Such approaches still involve trade-offs, including reduced liquidity and unequal capacity to commit resources.

Reputation-Based Governance

Reputation-based voting weights participation, work, expertise, or service to the community rather than financial holdings alone. This can broaden influence beyond token ownership, but reputation is not a naturally objective quantity. Poorly designed metrics may favor visible contributions over maintenance work, exclude newcomers, or allow coordinated groups to endorse one another. A credible reputation system therefore needs transparent criteria, contribution diversity, decay or review rules, appeals, and protections against a permanent insider class.

Smart Contracts And Transparency

Smart contracts can enforce eligibility snapshots, voting windows, quorum thresholds, timelocks, and execution rules. Public event logs help independent observers reproduce the governance record. Nevertheless, on-chain transparency does not eliminate off-chain coercion, bribery, compromised interfaces, oracle manipulation, private-key theft, or vulnerabilities in upgrade and execution logic. Governance security requires both protocol-level and social-process controls.

PROPOSED REPUTATION-BASED GOVERNANCE FRAMEWORK

The proposed model separates five components: contribution evidence, reputation computation, voting-power transformation, ballot administration, and proposal execution. The components should be modular so that the DAO can change parameters through a documented governance process rather than through discretionary intervention by a single administrator.

Page 70-82 © MANTECH PUBLICATIONS 2026. All Rights Reserved

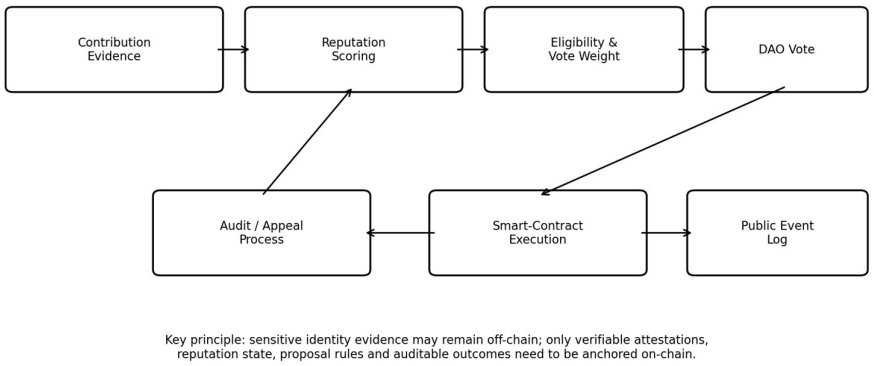


Figure 1: Proposed architecture for reputation-based DAO governance

Contribution Evidence And Reputation Dimensions

Reputation should not be a single popularity score. Candidate dimensions include verified code or documentation contributions, completed governance tasks, proposal analysis, community support work, security reporting, and participation in review processes. Each category should have published criteria and a method for contesting incorrect records. Self-reported activity alone should not produce substantial voting power.

Table: 1

Dimension	Possible evidence	Design safeguard
Technical contribution	Merged code, reviewed pull requests, reproducible bug reports	Quality review; avoid counting raw volume alone
Governance contribution	Reasoned proposal reviews, policy analysis, working-group outputs	Transparent rubric; plural reviewers
Community service	Documented support, onboarding, accessibility work	Recognize less-visible labor; periodic review
Security contribution	Validated vulnerability reports, completed audits	Responsible disclosure; avoid publicizing sensitive exploit details
Participation reliability	Attendance or completion of agreed tasks	Do not equate frequent activity with correctness or expertise

Page 70-82 © MANTECH PUBLICATIONS 2026. All Rights Reserved

Reputation Calculation

A candidate reputation score for member i at time t can be represented as a weighted sum of verified contribution categories with time decay:

$R_i(t) = \Sigma_k\, w_k \cdot q_{ik} \cdot e^{\wedge}(-\lambda_k \Delta t) - P_i(t)$

Here, w_k is the published weight for contribution category k; q_{ik} is the quality-adjusted verified contribution score; λ_k controls how quickly older contributions lose influence; Δt is the age of the contribution; and $P_i(t)$ represents penalties imposed after a documented, appealable finding of abuse. This expression is a conceptual specification, not a validated formula. Weights, decay rates, score bounds, and penalty rules require community deliberation and adversarial testing.

Reputation should be updated at defined intervals or governance epochs rather than immediately after every action. This reduces the opportunity to manufacture last-minute activity immediately before a snapshot. The system should also distinguish reversible reputation updates from irreversible contract execution.

Voting-Power Transformation

The framework recommends transforming reputation into bounded voting influence rather than using a direct one-to-one mapping. For example, a square-root or capped transformation may reduce marginal dominance by the highest-scoring members. A mixed model could combine a modest baseline participation component with a bounded reputation component, while avoiding a direct dependence on token wealth. Any formula must be tested for gaming, newcomer exclusion, and concentration.

$V_i = min(Vmax, \alpha + \beta\sqrt{R_i})$

This illustrative expression uses a baseline α, a reputation coefficient β, and an upper bound Vmax. It is not asserted to be optimal. If a DAO uses token ownership alongside reputation, the relative contribution of each component must be explicit, independently auditable, and subject to sensitivity analysis.

Page 70-82 © MANTECH PUBLICATIONS 2026. All Rights Reserved

Proposal And Voting Lifecycle

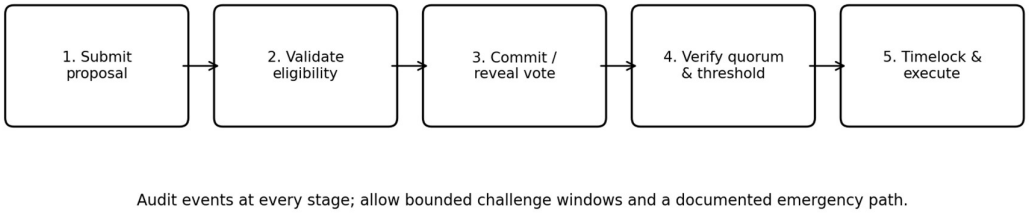


Figure 2: Proposal-to-execution lifecycle with audit and challenge points

Table: 2

Stage	Smart-contract or process rule	Audit evidence
Proposal submission	Require proposal format, proposer eligibility, and a minimum review window	Proposal ID, proposer address, timestamp, metadata hash
Eligibility snapshot	Freeze reputation inputs at a documented block or epoch	Snapshot reference and scoring version
Ballot opening	Enforce start/end times and one valid ballot per eligible voting credential	Ballot state transitions and voter-nullifier/credential checks
Vote tally	Apply published weighting, quorum, and approval threshold	Reproducible totals and rule version
Challenge period	Allow bounded challenges to eligibility or process defects	Challenge reason, evidence hash, resolution record
Timelock and execution	Delay consequential actions; provide a narrowly scoped emergency process	Execution transaction, delay, executor and event logs

Page 70-82 © MANTECH PUBLICATIONS 2026. All Rights Reserved

THREAT MODEL AND MITIGATION STRATEGY

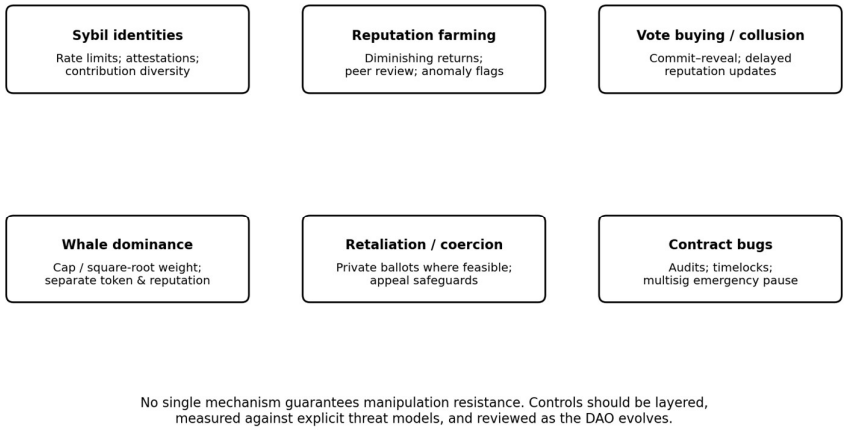


Figure 3: Common attack surfaces and candidate layered mitigations

Table: 3

Threat	Potential failure mode	Candidate controls	Residual limitation
Sybil attack	One actor creates multiple identities or credentials	Contribution attestations; rate limits; identity options where appropriate; credential revocation; cross-account anomaly review	Pseudonymous identities may remain linkable; central attestations can introduce gatekeepers
Reputation farming	Low-value actions are repeated to accumulate influence	Quality-adjusted scoring; diminishing returns; category diversity; delayed updates; peer review	Reviewers can collude and subjective scoring may be biased
Collusion / bribery	Participants coordinate votes or receive side payments	Commit–reveal ballots where suitable; delayed reputation updates; conflict disclosures; economic and behavioral monitoring	Commit–reveal does not prevent coercion or all forms of bribery

Page 70-82 © MANTECH PUBLICATIONS 2026. All Rights Reserved

Whale or insider dominance	A few members dominate due to wealth or accumulated status	Voting caps; nonlinear weights; reputation decay; newcomer pathways; concentration monitoring	Caps may reduce legitimate expert input; decay can undervalue long-term work
Proposal/interface manipulation	Ordering, framing, or author signals influence voter choice	Neutral proposal templates; balanced summaries; randomized option order where applicable; disclosure of authorship and conflicts	Interface effects cannot be removed completely
Smart-contract exploit	Bug or privileged upgrade changes votes or execution	Independent audits; unit/property tests; timelocks; constrained pause authority; staged deployment	Audits cannot prove absence of all defects
Privacy leakage	Public votes expose political or social preferences	Minimize on-chain personal data; privacy-preserving credentials; secret ballots where feasible	Privacy techniques increase complexity and may hinder public verification

TRANSPARENCY, PRIVACY, AND ACCOUNTABILITY

Transparency should apply to the rules and the integrity of the process, not automatically to personal identity. A DAO can publish scoring formulas, contract versions, proposal text, snapshot references, aggregate vote totals, challenge outcomes, and execution logs while limiting unnecessary disclosure of personal data. If ballots are public, the design should explicitly consider retaliation, coercion, and vote buying. If ballots are private, the DAO must explain how eligibility and tally correctness can still be independently verified.

A fair appeal process should define who may challenge a reputation update, what evidence is admissible, the response deadline, whether a reviewer has a conflict of interest, and how

Page 70-82 © MANTECH PUBLICATIONS 2026. All Rights Reserved

decisions can be appealed. Appeals must not become an unrestricted administrative override. Any emergency pause should be narrow, logged, time-limited, and followed by a public post-incident report.

EVALUATION PLAN AND PROPOSED METRICS

The framework should be evaluated before production deployment through a combination of formal analysis, simulation, testnet trials, and independent security review. The following are proposed measures, not results from an experiment conducted for this manuscript.

Table: 4

Evaluation domain	Suggested metric	Interpretation
Power concentration	Gini coefficient; Herfindahl–Hirschman index; top-1/top-10 voting share	Whether influence is concentrated among a small set of voters
Sybil resilience	Cost and success rate of simulated multi-identity attacks	How effectively the system limits identity multiplication
Collusion resilience	Outcome changes under coordinated voting and bribery assumptions	Sensitivity to organized manipulation
Participation	Turnout; first-time voter rate; participation by contribution category	Whether the design enables broad and sustained engagement
Reputation fairness	Score distribution; appeal reversal rate; newcomer time-to-eligibility	Whether reputation is contestable and accessible
Transparency	Independent reproduction of tally and execution history	Whether third parties can verify outcomes
Security	Critical/high findings; test coverage; invariant violations	Implementation quality and residual contract risk
Operational cost	Gas cost per proposal and ballot; latency	Practical feasibility at expected scale

Page 70-82 © MANTECH PUBLICATIONS 2026. All Rights Reserved

DISCUSSION

The central contribution of the proposed framework is not a claim that reputation alone solves DAO manipulation. Rather, it treats reputation as one governance input that must be bounded, auditable, time-sensitive, and challengeable. A layered architecture can make attacks more difficult and make irregularities easier to investigate, but the outcome depends on the threat model, membership structure, contribution evidence, and execution authority.

The design must avoid replacing plutocracy with an entrenched reputation oligarchy. Long-term contributors possess valuable institutional knowledge, yet newcomers and less-visible contributors also need credible routes to participation. Contribution categories should recognize maintenance, moderation, documentation, accessibility, and community support—not only code or public visibility. Reputation decay should be calibrated carefully: aggressive decay may discard durable expertise, while no decay can preserve obsolete influence.

A second trade-off concerns privacy. Fully public ballots maximize direct traceability but can enable coercion or strategic vote buying. Secret-ballot approaches may reduce these risks but add cryptographic complexity and require careful audit design. The choice should be proportional to the value at risk and the DAO's social context.

Finally, on-chain execution is only as safe as the contract and surrounding operational processes. Timelocks, independent audits, reproducible builds, role separation, and documented emergency procedures should be considered baseline safeguards for consequential governance actions.

LIMITATIONS

This is a narrative review and conceptual framework, not a systematic review or an empirical evaluation. The proposed equations and controls have not been calibrated against a specific DAO dataset. Security and fairness depend on assumptions that may differ across projects, and reputation evidence may be difficult to standardize across technical, social, and governance work. Privacy-preserving voting and identity-resistance techniques may add cost and usability burdens. The framework does not establish that a specific combination of controls is manipulation-proof.

Page 70-82 © MANTECH PUBLICATIONS 2026. All Rights Reserved

FUTURE SCOPE

- Implement a minimal prototype and publish the contract source, scoring rules, and threat model.
- Run adversarial simulations for Sybil creation, collusion, bribery, reputation farming, and strategic proposal timing.
- Compare token-weighted, capped-reputation, quadratic, and hybrid mechanisms using the same test scenarios.
- Conduct community-based usability studies to test whether scoring criteria are understandable and appeal processes are trusted.
- Evaluate privacy-preserving eligibility proofs and verifiable tally methods where public ballots pose coercion risks.
- Commission independent security audits and disclose limitations before handling treasury-level decisions.

CONCLUSION

Reputation-based DAO governance offers a promising route for broadening participation beyond financial ownership, but it is not inherently resistant to manipulation. A credible implementation should use transparent contribution criteria, quality-adjusted and time-sensitive reputation, bounded voting influence, clear snapshots, auditable voting rules, challenge procedures, timelocks, and layered security controls. The framework presented here is a research proposal whose value must be established through reproducible simulations, security analysis, and carefully governed pilots. It should not be described as proven or manipulation-proof until independent evidence supports those claims.

REFERENCES

1. Tamai S, Kasahara S. DAO voting mechanism resistant to whale and collusion problems. Frontiers in Blockchain. 2024;7. doi:10.3389/fbloc.2024.1405516.
2. Lalley SP, Weyl EG. Quadratic voting: How mechanism design can radicalize democracy. AEA Papers and Proceedings. 2018;108:33–37. doi:10.1257/pandp.20181002.
3. Lee J, Li T, Han J. Voting with Time Commitment for Decentralized Governance: Bond Voting as a Sybil-Resistant Mechanism. Management Science. Published online 2024. doi:10.1287/mnsc.2023.01536.

Page 70-82 © MANTECH PUBLICATIONS 2026. All Rights Reserved

4. Jungnickel M, Özdemir Sönmez F, Mulligan C, Knottenbelt WJ. DAO Governance: Voting Power, Participation, and Controversy—A Review and an Empirical Analysis. 2025. Preprint / working paper; verify final publication metadata before submission.
5. Han J, Lee J, Li T. A review of DAO governance: Recent literature and emerging trends. Journal of Corporate Finance. 2025;91:102734. doi:10.1016/j.jcorpfin.2025.102734.
6. Analyzing voting power in decentralized governance: Who controls DAOs? Blockchain: Research and Applications. 2024;5(3):100208. doi:10.1016/j.bcra.2024.100208.
7. Decentralizing governance: exploring the dynamics and challenges of digital commons and DAOs. Frontiers in Blockchain. 2025. doi:10.3389/fbloc.2025.1538227.
8. Voting Biases in Decentralized Autonomous Organization (DAO) Governance. arXiv preprint. 2026. arXiv:2607.09435.
9. Collusion-proof decentralized autonomous organizations. Research Policy. 2026;55(7):105509. doi:10.1016/j.respol.2026.105509.
10. OpenZeppelin. Smart Contract Security: recommendations and practices. Consult current official documentation and audit guidance before implementation.

***Author for Correspondence**
Shivani Bansal
E-mail: bansalshivani81@yahoo.co.in

[1,2,3]Students, Department of CSE, Supaul College of Engineering
[4]Professor, Department of CSE, Supaul College of Engineering

Received Date: July 03 2026
Accepted Date: July 15, 2026
Published Date: July 27, 2026

Citation: Shivani Bansal, Rituraj Rawat, Vandana Rajput, Abhishek Sharma. Reputation-Based Decentralized Governance Using Smart Contracts for Transparent and Manipulation-Resistant DAO Voting. Journal of Blockchain Systems and Smart Contracts. 2026; 2(2): 70-82p.

Page 70-82 © MANTECH PUBLICATIONS 2026. All Rights Reserved