ISSN (Online): 3139-7689

Available online: www.ijsrmes.com

International Journal for Scientific Research in Modern Engineering and Science

Published in Conference Special Issue: Vol. 1, Special Issue 1, pp. 374-384, 2026

A FUNCTIONAL CONTROL FRAMEWORK FOR ALLOCATING PREVENTING RESPONSIBILITY IN DECENTRALIZED AUTONOMOUS ORGANIZATION

Komal Meshram[1]*, Dilpreet Kaur[2], Md. Arshaan Khan[3], Danish Ahmed[3], Shankar Sharan Tripathi[4]

[1,2,3,4]Student, Computer Science and Engineering, Shri Shankaracharya Technical Campus
[5]Assistant Professor, Computer Science and Engineering, Shri Shankaracharya Technical Campus

Abstract

Decentralized Autonomous Organizations (DAOs) are blockchain-based governance systems designed to operate without centralized decision-making authority. Even though these systems are built to be decentralized, in practice, control is often shared among various groups through mechanisms such as token-based voting, administrative rights, and the ability to make system upgrades. This leads to a basic problem with accountability: when something goes wrong with governance or causes financial loss, it's hard to know who should be held responsible developers, those involved in governance decisions, or token holders. Most research looks at DAO liability through traditional legal frameworks or regulatory arguments, but there isn't a clear way to assess who should take preventive responsibility in these complex, multi-layered technical systems.

This paper offers a Functional Control Framework designed to clarify who should take preventive responsibility within DAOs. The framework looks at four important, observable factors: who can influence decisions, who has technical control, who recognizes or anticipates risks, and who stands to gain financially. Instead of merely accepting decentralization claims at face value, this model scrutinizes how power and responsibility manifest in practice. Using real-world examples, the paper shows that responsibility can shift depending on who has the capacity to control or prevent issues. By combining insights from both technical system design and legal principles of duty and control, this approach offers a clear, practical perspective on accountability in emerging decentralized systems—while ensuring that innovation re-mains encouraged.

Keywords: *Decentralized autonomous organization 1, functional control framework 2, preventive responsibility 3, accountability 4, governance mechanism 5, token-weighted voting 6, technical control 7, blockchain governance 8, financial loss 9, governance decision 10.*

* *Corresponding author*

1. Introduction

In 2016, one of the first large-scale decentralized investment experiments, known as "The DAO," lost about $60 million in cryptocurrency because of a smart contract flaw. The organization did not have a traditional CEO, board

of directors, or centralized management. However, when the exploit happened, the lack of central control did not remove the issue of accountability; it made it more urgent. If a decentralized system fails, who is responsible?

Decentralized Autonomous Organizations (DAOs) represent a new way of governance based on blockchain technology and automated smart contracts. Instead of using hierarchical management, DAOs embed operational rules into programmable code and allow collective decision-making through token-weighted voting. Early research describes blockchain governance as "rule by code," implying that automated enforcement might lessen dependency on institutions and spread authority among network participants. However, further studies warn that code-based governance does not remove human involvement; rather, it changes how that involvement works across technical design, gov-ernance participation, and economic incentives.

Even with claims of decentralization, real-world observations show that many DAOs still have imbalanced power structures. Administrative privileges, upgrade rights, multisignature controls, concentration of tokens, and front-end ownership can lead to functional centralization even within formally decentralized systems. This difference between having a decentralized structure and actual control becomes especially important when governance failures, financial losses, or regulatory actions occur.

Current literature mainly looks at DAO liability through comparisons to traditional corporations or regulatory frameworks. While these discussions focus on how entities are recognized and how limited liability protections work, they often treat DAO participants as if they are all the same. There has been little attention to organized methods for assessing preventive responsibility based on measurable control distri-butions.

This paper presents a Functional Control Framework for determining preventive responsibility in Decentralized Autonomous Organizations. The framework assesses accountability through four operational areas: technical authority, governance influence, knowledge and risk fore-sight, and economic benefit. By differentiating between formal decentralization and functional control, this study offers a clear way to allo-cate responsibility that connects legal duties with technical governance structures. Through case studies, the framework shows how ac-countability shifts across governance layers, creating a better understanding of responsibility in decentralized systems.

2. Conceptual Foundation and Research Gap

Formal decentralization has multiple definitions depending on the blockchain system and may be viewed from many perspectives. For ex-ample, formal decentralization can be described as the absence of a centralized governing body (the organization and/or individual), whereas functional control has to do with the division of power within a blockchain and may be characterized by administrative, governance, and economic control. A DAO may be structurally decentralized (no single identified leader/authority) and still have an overall functional cen-tralization of power if the authority to upgrade/modify the system and/or multisignature control and voting power to a small number of indi-viduals associated with that DAO remain intact; hence, when trying to determine responsibility, you must analyze the operational authority of the various members to ensure you are comparing apples to apples instead of comparing architectural types. From this point on, you will build your theoretical foundation.

In legal principles, responsibility is usually based on control and foresight. Individuals or groups that have the ability to make decisions or the means to stop harm are generally held to a higher duty of care. Negligence liability is based on the knowledge of risk and the ability to prevent that risk.

When you apply these principles to DAO systems, it can be inferred that those who have the ability to prevent an act should also have re-sponsibility for that act. If there are identifiable actors who have significant control despite the lack of any formal title or position within a managerial structure, then those actors are still considered to have responsibility.

While many of the current academic works are concentrating on blockchain governance or establishing a legal basis for DAOs' liabilities, there still remain several gaps in these areas.

First, most of the literature appears to address the issue of DAO's liability from a theoretical perspective with little known about how re-sponsibility could be measured within the multi-layered governance system.

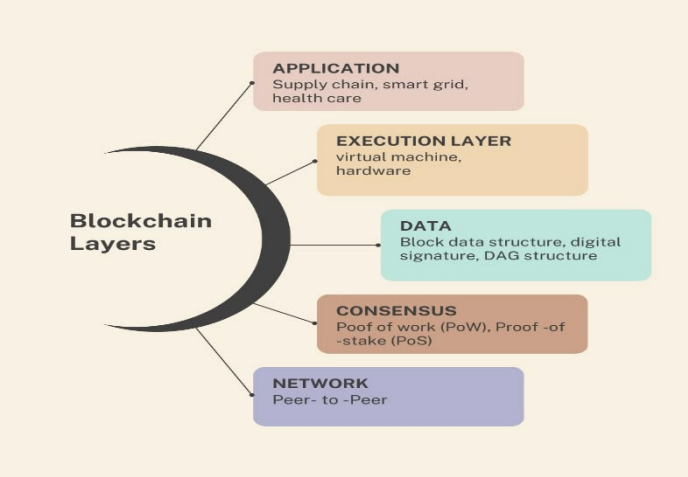

Fig. 1. Layered governance structure in decentralized autonomous organizations.

Second, most of the studies do not differentiate between different types of DAO participants as it appears that there is a widespread assump-tion that they all have the same degree of access to technical authority and to how much influence they exert in the governance of a DAO.

Thirdly, there are very few structured ways to assign preventative responsibilities to DAO members based on measurable distributions of the DAO's functional controls.

In general, because of this many of the analyses conducted to date on the accountability of DAOs are inconsistent, and do not rely on any systematic or empirical evidence, but rather tend to be based on broad generalized assump-tions.

To address this gap, a Functional Control Framework is proposed that outlines the responsibilities of DAOs using discrete measures of the technical authority, governance influence, risk knowledge and foreseeability, and eco-nomic benefit to determine the level of responsibility.

DAO governance distributes authority across multiple technical and governance layers, as illustrated in Fig. 1.

3. Functional Control Responsibility Framework

3.1. Normative Foundation

A basic normative principle underlies the functional control responsibility framework:

Where responsibility exists, so too should the ability to prevent something.

In legal theory, liability is often tied to control and foreseeability. Those in a position of control or with the ability to affect change will gen-erally have a higher level of duty of care than do those who lack such control. In decentralized systems of governance, authority is generally not contained in one office, but it is distributed across technical, governance, and economic layers. Consequently, accountability should be assessed according to functional control, rather than by organizational labels.

3.2. Structural Logic of the Framework

DAOs operate through layered governance mechanisms. Control within such systems can be categorized into four operational domains:

1. Technical Control (TC)
2. Governance Influence (GI)
3. Knowledge and Foreseeability (KF)
4. Economic Benefit (EB)

Each domain reflects a distinct dimension of functional authority. Responsibility intensifies when actors possess influence across multiple domains, particularly where prevention capacity and risk awareness intersect.

3.3. Responsibility Indicators

1. Technical Control (TC)

Technical Control measures the extent to which an actor can directly modify or intervene in protocol operations. Examples include:

- Administrative key possession
- Smart contract upgrade authority
- Emergency pause permissions
- Multisignature wallet participation

Actors with direct infrastructure authority possess immediate prevention capacity, increasing their responsibility exposure.

2. Governance Influence (GI)

Governance Influence measures an actor's ability to shape protocol outcomes through collective decision-making mechanisms.

This includes:

- Percentage of governance token ownership

- Voting dominance
- Delegated voting authority
- Proposal initiation privileges

Significant governance influence may determine whether risk-mitigating proposals are approved or rejected.

3. Knowledge and Foreseeability (KF)

This dimension evaluates whether an actor was aware, or reasonably should have been aware, of existing risks prior to harm.

Indicators include:

- Access to audit reports
- Publicly disclosed vulnerabilities
- Participation in governance discussions
- Technical expertise

Responsibility strengthens where risk was foreseeable and preventable.

4. Economic Benefit (EB)

Economic Benefit measures the extent to which an actor materially benefits from DAO operations.

Indicators include:

- Token allocation share
- Revenue participation
- Insider compensation
- Profit derived from governance outcomes

Financial alignment with system outcomes may amplify responsibility when combined with control or knowledge.

3.4. Responsibility Scoring Structure

Each indicator is evaluated on a 0–3 scale:

0 – No measurable influence

1 – Limited influence

2 – Moderate influence

3 – Significant influence

Total Responsibility Score:

$R_i = TC_i + GI_i + KF_i + EB_i$

Where R_i represents the preventive responsibility intensity of actor i.

Classification:

0–3 → Low Responsibility

4–7 → Moderate Responsibility

8–12 → High Responsibility

This scoring structure is not intended to assign legal liability but to provide a structured analytical tool for pro-portionate accountability as-sessment.

3.5. Dynamic Responsibility Principle

Within Decentralized Autonomous Organizations (DAOs), responsibility is always on the move — it will shift responsibility dynamically based upon who's actually capable of doing something to prevent harm at the moment that it occurs. For example, if a developer retains control or has the ability to upgrade protocols (which will affect the allocation of responsibility), the developer will therefore have a signifi-cant amount of control over how re-sponsibilities are allocated relative to those under governance voting authority (i.e., who controls the protocol). Likewise, as a result of the above examples, accountability must also be evaluated in context and across various layers of govern-ance.

3.6. Operational Application Procedure

The framework may be applied through the following steps:

1. Identify relevant actors involved in governance or protocol design.
2. Determine each actor’s position within the layered control structure.
3. Evaluate the four responsibility indicators.
4. Compute Responsibility Score.
5. Classify preventive responsibility level.

This structured process enhances analytical clarity while maintaining flexibility for diverse DAO configurations. The Functional Control Responsibility Framework evaluates accountability through a structured process illus-trated in Fig. 2.

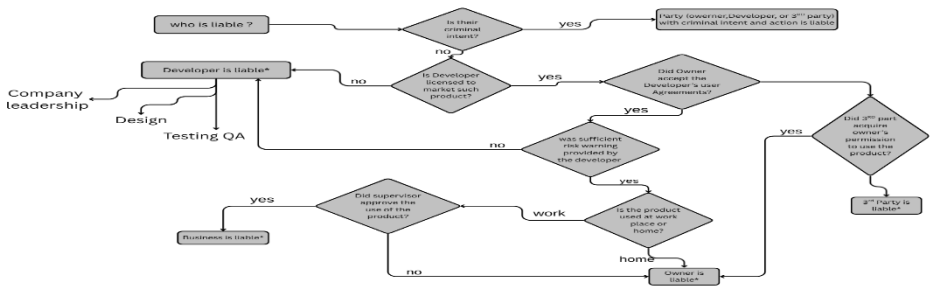

Fig. 2. Functional control responsibility evaluation process.

4. Case Study Application

A. Case Study 1: The DAO Hack (2016)

4.1. Background

In 2016, one of the very first "DAOs" (Decentralized Autonomous Organizations) was created and deployed on Ethereum's blockchain as an investment fund. The protocol used smart contracts to pool capital from multiple sources and governed activity through a voting process by token-holders.

When the DAO was initially launched, a recursive method to withdraw funds from the smart contracts resulted in the loss of approximately $60 million worth of cryptocurrency.

While there were no centralized executives managing the activities of the DAO, the incident raised significant questions about how to hold different parties accountable for the loss. Because the DAO's structure did not provide for a traditional corporate hierarchy, there was con-siderable ambiguity about which participants in the decentralized governance structure had an ability to (1) prevent the loss from occurring or (2) mitigate the impact of the loss on affected parties.

The circumstances surrounding this case make it a suitable opportunity for applying the Functional Control Responsibility Framework.

4.2. Actor Identification

For analytical clarity, three primary actor categories are evaluated:

1. Core Developers
2. Major Token Holders (Governance Whales)
3. Small Investors / Passive Participants

Each actor category is assessed across the four responsibility indicators: Technical Control (TC), Governance Influence (GI), Knowledge & Foreseeability (KF), and Economic Benefit (EB).

4.3. Responsibility Evaluation

(a) Core Developers

Technical Control (TC): 3

Developers designed and deployed the smart contract infrastructure.

Governance Influence (GI): 1

Limited direct dominance in voting mechanisms.

Knowledge & Foreseeability (KF): 3

The recursive withdrawal vulnerability was a foreseeable technical risk under known smart contract patterns.

Economic Benefit (EB): 2

Developers had indirect financial exposure through token allocation or ecosystem incentives.

Total Responsibility Score:

$R = 3 + 1 + 3 + 2 = 9$

Classification: High Responsibility

Interpretation:

Developers possessed both technical authority and risk awareness, indicating substantial prevention capacity.

(b) Major Token Holders

Technical Control (TC): 1

No direct authority to modify smart contracts.

Governance Influence (GI): 3

Significant voting power capable of influencing governance outcomes.

Knowledge & Foreseeability (KF): 2

Access to public governance discussions and technical disclosures.

Economic Benefit (EB): 3

Substantial financial stake in protocol performance.

Total Responsibility Score:

R = 1 + 3 + 2 + 3 = 9

Classification: High Responsibility

Interpretation:

Governance dominance combined with financial interest indicates strong accountability exposure.

(c) Small Investors / Passive Participants

Technical Control (TC): 0

No authority over infrastructure.

Governance Influence (GI): 1

Minimal voting impact.

Knowledge & Foreseeability (KF): 0

Limited technical awareness of vulnerabilities.

Economic Benefit (EB): 1

Small financial participation.

Total Responsibility Score:

R = 0 + 1 + 0 + 1 = 2

Classification: Low Responsibility

Interpretation:

Limited prevention capacity and minimal governance influence result in proportionately low responsibility.

5. Results and Discussion

5.1 Key Findings

An analysis of the application of the Functional Control Responsibility Framework to the DAO hack and the rejected governance scenario indicates a number of consistent patterns.

Using Decentralization as an example, it is clear that decentralization does not eliminate individuals from being held accountable. The ab-sence of any centralized executive(s) means that functional control of the organisation will continue to be distributed amongst all of the iden-tifyable actors. This means that regardless of Decentraliza-tion, accountability remains engaged with actors in proportion to their capacity for prevention.

Where an actor has technical authority, the degree that they will be exposed to accountability will increase signif-icantly. For example, if an individual has upgraded permissions, or has administrative keys, or has the ability to intervene in an emergency, they'll be expected to demonstrate additional preventive duty due to their ability to eliminate risk directly.

In addition, Governance has a major impact on the allocation of responsibility for the organisation's activities. This is because an actor will use the ownership of a concentration of tokens to influence security decisions, ap-prove or reject a mitigation plan, and/or indirectly affect the stability of the protocol.

In addition, knowledge and foreseeability will increase an actor's accountability. When a vulnerability is made available for public disclosure or is reasonably discoverable, every actor that has expertise in the subject matter or has access to governance will have increased accounta-bility.

Finally, passive participants with no significant influence and/or limited knowledge will generally have a propor-tionately lower level of re-sponsibility for the organisation's activities. The framework provides a means to dif-ferentiate between actors based upon the level of quanti-fiable control rather than on a basis of uniform classifi-cation.

5.2 Theoretical Implications

The data reinforce the difference of formal and functional decentralization. Decentralized DAOs often have an operational layer of authority that has control. This means that an organization's responsibilities will be based on their functional role or influence vice their structure (con-struction).

The prevention of harm between the duties of governance and the foreseeability of damage is made possible by defining prevention ability as the main criteria of who will be held liable for damages.

5.3 Practical Implications

Regulators and policymakers should allocate responsibility in decentralized systems proportionately, not abso-lutely. Blanket immunity could undermine user protection, whereas blanket liability could discourage innovative development of decentralized systems.

Utilizing a structured and control-based approach can help provide accountability for evolving blockchain eco-systems in a fair manner.

6. Limitations

While the Functional Control Responsibility Framework provides an organized system to distribute preventive responsibility for DAO sys-tems, there are some recognized limitations of the methodology.

To start, the scoring mechanism relies on subjective judgment. The indicators are defined very well, however assigning actual numerical values of 0-3 may be different depending on the information available and the perspective of the analyst. As such, the framework is not a definitive formula for the purpose of liability, but rather an evaluative tool.

Secondly, the framework assumes a reasonable amount of transparency exists in DAO governance structures. However, in reality, issues such as the concentration of token ownership, multisign control, or informal cooperation between participants may not be apparent to the public. As such, the lack of available data may hinder the ability to accurately determine prevention responsibilities.

Third, the functional controls responsibility framework does not replace formal legal adjudication. It is meant to provide a structured, analyt-ical framework for evaluating the capacity to prevent, but the actual determination of liability is determined by regulations, laws and amount of evidence relevant to the residential jurisdiction.

Fourth, this study will use the framework on a conceptual basis with a case study design instead of large-scale empirical analysis. Future research could validate the model through quantitative analysis of several incidents of DAO governance.

Despite these limitations, the Functional Controls Responsibility Framework provides a coherent basis for evaluating accountability in a decentralized governing structure.

7. Conclusion

DAOs embody a significant transformational step in digital governance and present a challenge to traditional notions of hierarchy, authority, and accountability. Although DAOs are often viewed as decentralized systems that function without any central authority, the actual applica-tion of DAOs often results in a layered distribution of functional control. Even though there may be no formal executives within DAOs, there is still a redistribution of capacity to prevent problems among various domains including technical, governance, and economic areas.

A clear gap exists in the various literature regarding a structured methodology for allocating preventive accountability within decentralized entities; so, the Functional Control Responsibility Framework proposed by this study refers to accountability as being based on four meas-urable dimensions: 1) technical control, 2) governance, 3) knowledge and foreseeability of risk, 4) and economic benefit.

The application of the Functional Control Responsibility Framework to case studies demonstrated that responsibility exists within DAOs in a dynamic and proportional manner. This means that depending on the time of loss/damage, the actors in possession of the most meaningful ability to prevent the loss/damage can change. These findings indicate that the process of decentralization does not remove the responsibility, but rather restructures the responsibility within a more layered governance structure.

This research provides a structured and balanced approach to the allocation of responsibility in decentralized systems by integrating the legal concepts of the principles of control and foreseeability with the technical analysis of governance. Ultimately, the enhanced evolution of blockchain-based governance systems may lead to innovative solutions through the use of accountability frameworks based on proportion-ate and control principles.

References

[1] Saurabh, K. (2024). Towards novel blockchain decentralized autonomous organization–led corporate governance. Tech-nological Forecasting and Social Change.

[2] Sarkar, D., & Arora, C. (2024). Web3 and the state: Indian state's redescription of blockchain.

[3] Government of India – NITI Aayog. (2018). Blockchain: The India strategy (IndiaChain initiative).

[4] Hassan, S., & De Filippi, P. (2021). Decentralized autonomous organization. Internet Policy Review

[5] Siegel, D. (2016). Understanding the DAO attack. CoinDesk.

[6] De Filippi, P., & Wright, A. (2018). Blockchain and the law: The rule of code. Harvard University Press.

[7] Werbach, Kevin. (2018). The Blockchain and the New Architecture of Trust. MIT Press.

[8] DuPont, Quinn. (2017). Experiments in Algorithmic Governance: A history and ethnography of "The DAO," a failed de-centralized autonomous organization. In Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance. Routledge.

[9] Buterin, Vitalik. (2016). Critical Update Re: DAO Vulnerability. Ethereum Foundation Blog.

[10] Jentzsch, Christoph. (2016). Decentralized Autonomous Organization to Automate Governance

[11] Saito, Y., & Rose, J. (2022). Reputation-based decentralized autonomous organization for the non-profit sector. Frontiers in Blockchain.

[12] Rikken, O., Janssen, M., & Kwee, Z. (2019). Governance challenges of blockchain and decentralized autonomous organi-zations.

[13] Patil, R., Swarnkar, S. K., Bhadane, D. Y., Poddar, G. M., Patil, M. P., & Sonawane, R. C. (2025). Exploring governance frameworks and decision processes in blockchain-based decentralized autonomous organizations. International Journal of Basic and Applied Sciences.

[14] Khare, P. A., Sonawane, V. R., Chopade, S. M., Sapkale, B. B., & Patil, D. D. (2025). Decentralized autonomous organiza-tions for governance and operations. International Journal of Creative Research Thoughts (IJCRT).

[15] Kolber, A. (2018). Not-so-smart contracts. Georgetown Law Technology Review.