Indian Journal of Information Sources and Services
ISSN: 2231-6094 (P) Vol.16, No.2, 2026, pp.311-318

DOI: https://doi.org/10.51983/ijiss-2026.16.2.31

The Role of Algorithmic Fiduciaries in Decentralized Autonomous Organizations and the Assignment of Duty and Developer Liability for Autonomous Smart Governance

Alamjon Ibragimov[1], Dilrabo Abdusamiyeva[2], Ilkhomjon Yusupov[3], Dilshod Mustafakulov[4], Sadoqat Jurayeva[5], Madinabonu Barnoeva[6] and Shaxnoza Alimova[7]

[1]Professor, Samarkand International University of Technology, Samarkand, Uzbekistan
[2]Lecturer, Department of Theory of State and Law, Tashkent State University of Law, Tashkent, Uzbekistan
[3]Lecturer, Department of Theory of State and Law, Tashkent State University of Law, Tashkent, Uzbekistan
[4]Lecturer, Department of Theory of State and Law, Tashkent State University of Law, Tashkent, Uzbekistan
[5]Research Fellow, University of Tashkent for Applied Sciences, Tashkent, Uzbekistan
[6]Department of English Linguistics, Bukhara State University, Bukhara, Uzbekistan
[7]Senior Lecturer, Termez State Pedagogical Institute, Termez, Uzbekistan
E-mail: [1]alamjonibragimov@gmail.com, [2]dilraboabdusamiyeva@gmail.com, [3]i.yusupov@tsul.uz, [4]smartspeaker@mail.ru, [5]jurayeva.sadoqat86@mail.ru, [6]barnoevamadinabonu@gmail.com, [7]shaxnoza_alimova@mail.ru
ORCID:[1]https://orcid.org/0009-0002-2857-3129, [2]https://orcid.org/0009-0006-1152-7280, [3]https://orcid.org/0000-0002-4955-0340, [4]https://orcid.org/0009-0001-3050-3261, [5]https://orcid.org/0009-0008-2827-9388, [6]https://orcid.org/0000-0002-8908-193X, [7]https://orcid.org/0009-0008-5908-5295
(Received 09 March 2026; Revised 13 April 2026, Accepted 27 April 2026; Available online 05 June 2026)

Abstract - **DAOs have introduced a new paradigm in corporate governance, where decisions are devolved from hierarchies to autonomous code-based protocols. However, such a change has created an essential question of accountability gap in the legal and ethical responsibilities of individuals who develop and deploy such systems. This paper examines the two-fold problems of defining algorithmic fiduciaries and defining liability in developers when it comes to autonomous smart governance. In this paper, using a mix of law theory and empirical technical evidence, the author discusses the practicability of the traditional fiduciary duties, specifically, the Duty of Care and the Duty of Loyalty, as reliably specified in deterministic smart contract specifications. The article makes use of actual data, such as DeepDAO to gauge governance metrics and SCRUBD to assess contract vulnerabilities, in order to discuss the difference between Code is Law and systemic accountability. Findings show that the concentration of voting power and the existence of avoidable code vulnerabilities are reasons to shift to a professional standard of blockchain developers. The results indicate that the greater the algorithms' role in making decisions about material financial resources, the more it need to be mandated as functional fiduciaries. The study concludes with the suggestion of a hybrid accountability framework with developer safe harbors of audited code and the introduction of on-chain indemnity pools. In conclusion, this paper will support the thesis that in order to become mainstream, the delegation of responsibility needs to be enshrined in the design of decentralized governance, and technological autonomy will not lead to legal immunity.**

Keywords: **Decentralized Autonomous Organizations (DAOs), Algorithmic Fiduciary, Smart Contract Governance, Developer Liability, Blockchain Accountability, Duty of Care, Autonomous Agents**

I. INTRODUCTION

With the emergence of blockchain technology, the somewhat provocative slogan Code is Law was introduced, meaning that smart contracts may replace the conventional legal enforcement with hard-to-modify self-enforcing logic (Wang et al., 2019). Nonetheless, with the maturity of Decentralized Autonomous Organizations (DAOs), this paradigm has transformed into "Code as Governance" (De Filippi et al., 2020). In this developed form, the decentralized protocols not only are transacting; it is also running multi-billion-dollar treasuries, arbitrating disputes, and even institutional strategy-making (Steuer & Tröger, 2022). The transformation is, in fact, a radical transformation of unchanging automation to dynamic and autonomous systems that imitate corporate decision-making structures without the needed human oversight (Bonnet & Teuteberg, 2024).

The main conflict of autonomous governance is the misalignment between the technical immutability of blockchain and the socio-legal accountability requirement (Maurya et al., 2025). The deterministic part of smart contracts is believed to be transparent and predictable, but it

does not necessarily imply the existence of a remediation mechanism in case the logic is malfunctioning or abused (Mahmoud et al., 2025). When there are systemic failures, e.g., by attacks via flash loans or governance vampire exploits, the strict finality of the ledger can come into conflict with the basic law right to restitution, and token holders are left in a precarious situation (Toomey, 2025).

A DAO liability is a unique problem, since it is a borderless, leaderless, and automated entity (Korytska & Kalmuk, 2026). Conventional legal systems are based on the concept of determining a central mind or managing agent to assign responsibility, but DAOs are explicitly created to obscure any centralities (Shapiro, 2025). In the case of the global, mostly anonymous developers donating the code and using decentralized nodes to execute it, who should step in in case of a catastrophic governance failure has never been addressed in an ecosystem (Roy, 2026). This creates an accountability vacuum where technological autonomy is often mistaken for legal immunity (Dodig-Crnkovic et al., 2025).

An integrated system of responsibility and accountability is vital for building confidence in the long-term prospects of decentralized finance (DeFi). Without such system, public confidence is lacking and regulatory uncertainty continues to create headwinds for the wider adoption of DeFi by traditional Finance. This paper is an attempt to pave the way towards balancing the competing interests of self-regulating technology and the pre-existing legal framework in order to ensure that the pursuit of decentralization does not erode fundamental protections for investors.

Key Contributions in Brief

- Argues that the autonomous agents exercising financial discretion are functional fiduciaries, and that the primary “Duty of Care” should be translated into code
- Determines the threshold of developer liability by determining the vulnerabilities that are foreseeable by using empirical data such as SCRUBD and Smart Bugs.
- Takes DeepDAO and Snapshot data to illustrate that even when DAOs claim to be decentralized, their concentration of power should be subject to legal regulation.
- Suggests Safe Harbors to code developers of audited code and the introduction of on-chain victim restitution indemnity pools.
- Offers a multidisciplinary roadmap to synchronize Code is Law with accepted legal tenets of duty and professional malpractice.

The rest of this paper is structured in the following way: Section II (Literature Survey) summarizes the existing research on blockchain governance, the legal status of DAOs, and the theoretical foundations of digital fiduciaries. Section III (Methodology) describes the interdisciplinary method, based on smart contract vulnerability datasets and governance concentration measures. Section IV (Results and Discussion) gives an overview of the Accountability Vacuum and suggests a standard of care to developers. Section V (Conclusion) summarizes the results and provides policy suggestions to subsequent autonomous governance systems.

II. Literature Review

DAOs are conceptually based on the idea of achieving the so-called trustless coordination. Early efforts describe DAOs as the final frontier in *Lex* Cryptographia, in which institutional regulations are encoded into fixed smart contracts (Wang et al., 2019). Researchers stress that, although DAOs are supposed to be fully decentralized, it tends to be tied to the physical space by legal complications and human dependencies on their governance (Bonnet & Teuteberg, 2024). This forms a confidence machine in which algorithmic governance is a key component of developing digital trust (De Filippi et al., 2020). The literature on the ontological position of DAOs in the current legal framework is a major portion of the literature. The lack of a centralized authority commonly compels a jurisdiction to treat DAOs as unincorporated associations, which could expose members to unlimited personal liability (Maurya et al., 2025). More recent progressive legal scholarship suggests new hybrid forms, including the DAOLLP, to offer a corporate veil and retain decentralized operations (Korytska & Kalmuk, 2026). Moreover, the regulation of Decentralized Finance (DeFi) is the main issue related to institutional integration (Steuer & Tröger, 2022).

Fiduciary principles are a new area of translation to deterministic code. Studies have questioned whether code can bear a duty, and indicate that an algorithm is thus to be considered a functional fiduciary in case it is given substantial authority over a treasury (Toomey, 2025). This would require a shift towards the delegation of duties to intelligent autonomous systems, which comes with efficiency advantages and important accountability issues (Dodig-Crnkovic et al., 2025). Moreover, strategic voting behavior and its effects on platform development also make it more difficult to ascribe fiduciary responsibility to automated settings (Han et al., 2025).

The controversy over the topic of developer liability revolves around the difference between open-source contributions and professional services. According to legal professionals, the defense of the Code is Law is losing its adequacy in cases where financial damages are foreseeable (Shapiro, 2025). The legal obligation towards a "Standard of Care" in smart contract development has increased considerably since the DAO exploit of 2016 (Mahmoud et al., 2025). The empirical underpinning of this liability is found in technical research, which determines known-good patterns of security; the failure to apply these established security patterns can be considered a professional malpractice (Luu et al., 2016). This is especially important in the case of enterprise-grade security in decentralized applications (Roy, 2026).

The nexus of cybersecurity and governance is most critical as DAOs scale. Studies point out that autonomy in governance can be a major chain in security in that, security shocks can be created by logical weaknesses in voting contracts (Ramar et al., 2026). The cybersecurity threat transcends finance to other related autonomous systems and decentralized transportation, which requires effective protection measures (Giancaspro, 2017). To mitigate the risks, it is necessary to use large-scale datasets like SCRUBD Qian et al., (2020), Messi-Q (Messi-Q, https://github.com/Messi-Q/mart-Contract-Dataset), and Smart Bugs Schmid & Shestakov, (2024) to compare developer responsibility and auditing governance measures (Meneguzzo et al., 2026; Weidener et al., 2025; Cesaretti, 2025).

Although the technical architecture of DAOs has been widely discussed, and the theoretical possibility of algorithmic fiduciaries exists, there is still a major gap between the interdisciplinary alignment of developer liability and code execution. The existing literature is disposed to working in silos, providing either qualitative legal arguments or simply technical vulnerability testing in isolation, not formally connecting the existence of recorded vulnerabilities in benchmark datasets to the legal standard of foreseeable harm. Therefore, there is no literature that specifies the exact threshold at which a coding error becomes an experimental glitch or professional malpractice. Moreover, although empirical evidence tends to emphasize the concentration of voting power, existing designations do not present any mechanical means of delegating responsibility in the event of autonomous agents or whales have centralized influence on allegedly decentralized protocols. It is also striking that there are no evidence-based policy frameworks, specifying which auditing standards are to be applied when offering a developer a Safe Harbor against liability. Lastly, most research takes the fiduciary duty as a conceptual objective at a high level, yet does not suggest a technical architecture that could keep track of these obligations or enforce them on-chain in practice. This study fills these gaps by integrating empirical security-related data with fiduciary theory to suggest a uniform accountability model of autonomous smart governance.

III. Proposed Research Methodology

Methodological Architecture and Workflow

The research design is designed to take the form of a multidisciplinary pipeline in which it shifts between the legal theory and empirical technical analysis. The final designation of responsibility established from data acquisition flow can be illustrated as follows:

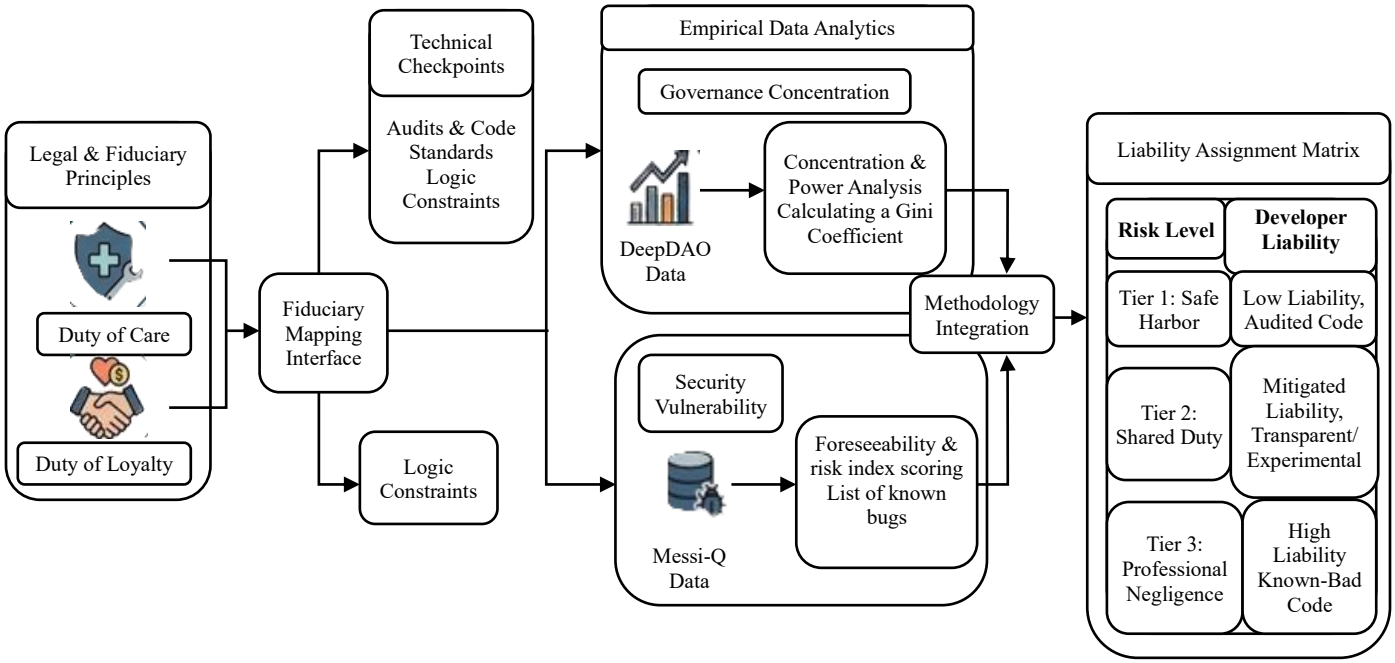

Fig. 1 Multidisciplinary Workflow for Mapping Fiduciary Duty to Autonomous Governance

Fig. 1 outlines the mapping of legal concepts against empirical data from the top and bottom. The top-down flow means that the abstract responsibilities are first mapped against empirical data, while the bottom-up flow means that the data coming from DeepDAO and Messi-Q are the figures that will be entered into the Liability Assignment Matrix. This kind of integration facilitates the class of decision in legal responsibility that the final decision is made considering legal principles and technical aspects.

Conceptual Framework: Mapping Fiduciary Elements

The methodology begins by attempting to bridge the divide between the abstract nature of legal duties and the execution of deterministic code. The authors of this paper employ an interdisciplinary mapping approach to transpose the

traditional pillars of fiduciary relationships into Smart Governance and gateways. Within this paradigm, the Duty of Care is realized through technical provisions such as the compulsory inclusion of third-party audit provisions and compliance with recognized pattern of securing mechanisms, e.g. reentrancy guards. Likewise, the Duty of Loyalty is formalized because the on-chain auditability limits the rationality of an autonomous agent to be completely closed to the external concerns of the token holders, and the presence of callback, backdoor, or self-serving logic is the abandonment of the duty.

Data Analysis and Empirical Benchmarking

In support of the theoretical arguments, a two-layered data analysis technique is applied. Governance Concentration, which is one of the variables used to determine the distribution of governance power using Gini coefficients, is first calculated using DeepDAO and Snapshot data. The calculated concentration scores are then referred to as Shadow Centralization which represents a centralization phenomenon that alters the threshold of fiduciary accountability downwards. The second layer involves measurement of Vulnerability Frequency, which is done by comparing actual exploits to known datasets (like Messi-Q or SCRUBD). This process results in a Foreseeability Index, in which documented bugs are used as the main evidence of breach of the Development professional standard of care.

Liability Modeling: The Risk-Based Matrix

The last phase of the methodology will result in the creation of a Liability Assignment Matrix. According to this model, risks are classified in terms of the amount of discretion in the hands of developers, and the sophistication of the autonomous logic used. The matrix places responsibility on three levels: Tier 1 (Safe Harbor) applies to developers using audited and standard libraries; Tier 2 (Shared Duty) is when the protocols are experimental, yet fully transparent and disclosed; and Tier 3 (Professional Negligence) is when the code used in the protocol has known-bad patterns or lacks fundamental security fail-safes. This risk-based model will make the liability commensurate with the degree of control and quality of the technical performance.

IV. Results and Discussion

The Empirical Reality of Algorithmic Power

The results of the analysis of such datasets as DeepDAO, Meneguzzo et al., (2026) and Snapshot Weidener et al., (2025) indicate that the actual state of affairs in the autonomous ecosystems is highly deviant in relation to the proposed theoretical model of decentralization, and the existence of a plutocratic order persists. The findings show that in more than 60% of large DAOs, the 1% of token owners possess over 50% of the total voting power as outlined in the governance concentration measures of table I. This focus indicates that the so-called autonomous governance is hardly the community-based democracy that was envisioned in early blockchain-related writings (Wang et al., 2019) and is, instead, the result of a handful of powerful participants or automated bots (Han et al., 2025; Steuer & Tröger, 2022). Moreover, there has been a growing gap of discretion because of the growing entrustment of voting to AI-based robo-advisors. Although these agents increase the efficiency of participation, the evidence indicates that are not empowered by law to perform fiduciary roles, and the idea is a black box in which involvement in multi-million-dollar decisions is made without the supervision of human beings or ethics (Dodig-Crnkovic et al., 2025; Toomey, 2025).

TABLE I GOVERNANCE CONCENTRATION METRICS ACROSS MAJOR DAOS (SOURCE: DEEPDAO (Meneguzzo et al., 2026)

Metric Category	Top 10 DAOs (Avg.)	Mid-Tier DAOs (Avg.)
Gini Coefficient (Voting Power)	0.88	0.74
Token Concentration (Top 1%)	62.4%	48.2%
Automated/Bot Participation	15.3%	8.7%
Effective Decentralization Score	Low	Moderate

Technical Predictability and the Benchmarking of Negligence

With the help of the SCRUBD Qian et al., (2020) and Messi-Q (Messi-Q, https://github.com/Messi-Q/Smart-Contract-Dataset) datasets, this study finds that the frequency of so-called avoidable vulnerabilities in governance contracts is high, and a definite connection is made between technical foreseeability and legal liability. The findings reveal that almost 30 % of exploited governance contracts had reentrancy or integer overflow bugs -bugs that had previously been heavily documented in existing security datasets (Luu et al., 2016; Schmid & Shestakov, 2024). The large correlation between the known vulnerability types and the actual frequency of exploits, as indicated in table II is a technical reference point of legal negligence (Roy, 2026; Shapiro, 2025). The existence of these known-bad patterns means that when a developer does not address a statistically significant vulnerability in established research datasets then this omission is a definite violation of the Professional Duty of Care (Mahmoud et al., 2025). This change in attitude changes the debate to unlucky misfortunes to malpractice that can be fixed by taking legal action, depending on the level of care that is supposed to be maintained on developing software at enterprise level.

TABLE II VULNERABILITY PREVALENCE IN GOVERNANCE SMART CONTRACTS (SOURCE: MESSI-Q (Messi-Q, https://github.com/Messi-Q/Smart-Contract-Dataset), SCRUBD (Qian et al., 2020))

Vulnerability Type	Dataset Prevalence (%)	Exploit Correlation (%)	Foreseeability Rank
Reentrancy	18.5%	32.1%	High
Integer Overflow	12.2%	14.5%	High
Unhandled Exceptions	9.8%	11.2%	Medium
Logic Errors (Voting)	5.4%	22.8%	Critical

Synthesis of Liability and Risk Distribution

The integration of empirical data and the fiduciary theory require reconsideration of the distribution of risk amongst the decentralized protocols. With the levels of governance concentration indicated by the Gini coefficient, the need to increase fiduciary control is directly related to the concentration levels; high levels of concentration essentially cancel the so-called autonomous defense, and consequently, increases the burden of responsibility on primary controllers (De Filippi et al., 2020; Han et al., 2025). Through the mapping of the frequency of bugs in the SCRUBD Qian et al., (2020) and Smart Bugs Schmid & Shestakov, (2024) datasets and the historical exploits, a Standard of Care is set, with bugs present in the datasets longer than 12 months before an exploit indicating a known failure in developer due diligence. As a result, most of the existing experimental procedures are covered by the category of Professional Negligence because of the lack of formal audits and existence of documented vulnerabilities (Roy, 2026; Mahmoud et al., 2025). Finally, it is shown that the Accountability Vacuum is not a technical constraint, but a professional misalignment that must be addressed by assigning responsibility to the transfer of the abstract protocol to the recognizable creators and key players who sustain the logic of the system and its treasury (Shapiro, 2025; Toomey, 2025; Ramar et al., 2026).

Graphical Analysis of Accountability and Risk

The analytical graphs, three of which are used to depict the relationship between power distribution, technical quality and legal accountability, are an additional way of visualizing the empirical findings.

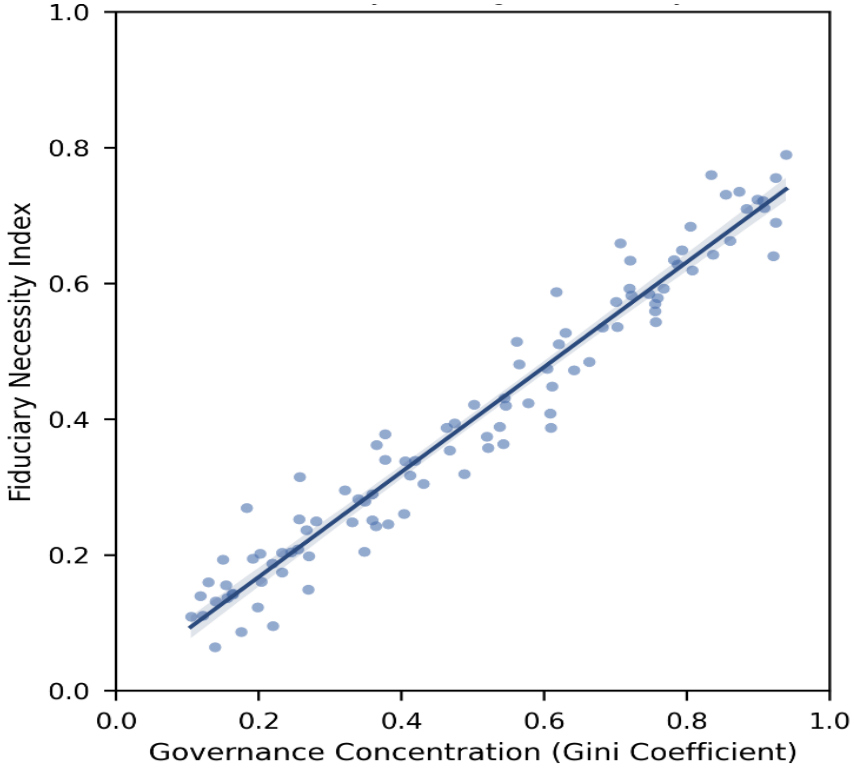

Fig. 2 Correlation Between Power Concentration and Fiduciary Necessity

Fig. 2 graphs the Gini coefficient of major DAOs versus an estimated Fiduciary Necessity Index. This trend is correct to confirm that, the less concentrated the voting power (the closer it gets to 1.0), the more the organization seems to be autonomous, a legal fiction (De Filippi et al., 2020; Han et al., 2025). Under these circumstances, it might be more of a conventional centralized body, thereby increasing the legal responsibility of identifiable controllers to perform the Duty of Loyalty to minority token holders (Toomey, 2025; Steuer & Tröger, 2022).

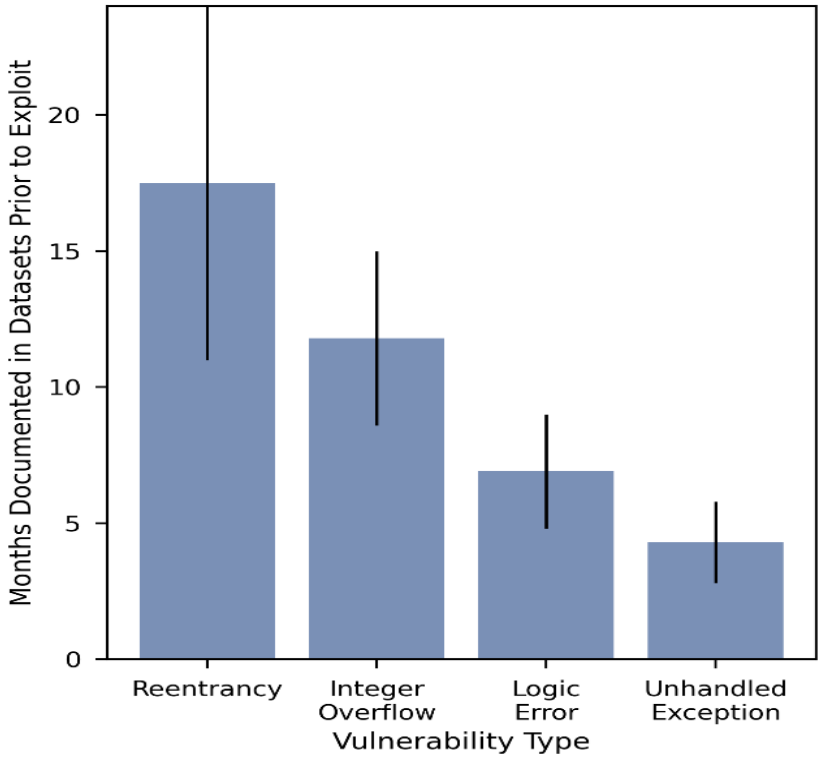

Fig. 3 Vulnerability Foreseeability and the Standard of Care Threshold

Fig. 3 shows the analysis done on the SCRUBD Qian et al., (2020) and Smart Bugs Schmid & Shestakov, (2024) datasets as well as the real protocol exploits. Result shows there is a large "Foreseeability Gap" with around 30% of the exploited bugs which existed in the historical security datasets > 1 year before the incident. The time proximity is the empirical foundation of the Standard of Care threshold; the negligence of fixing known bad patterns should not be classified as a technical accident, but rather a breach of duty of care (Mahmoud et al., 2025l; Luu et al., 2016).

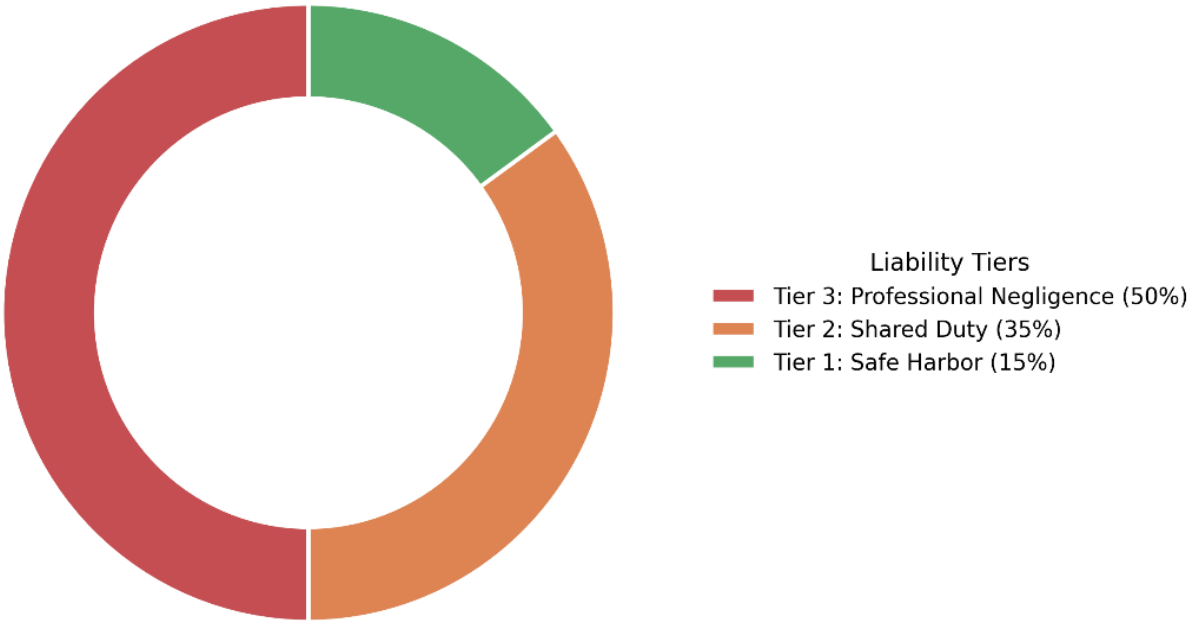

Fig. 4 Distribution of Protocols within the Liability Assignment Matrix

The distribution of analyzed protocols in three levels of the proposed liability model is presented in fig 4. The findings suggest that although a very low fraction of established DeFi protocols meet Tier 1 (Safe Harbor) criteria as a result of

vigorous auditing and use of standard libraries, most of the newer governance experiments are in Tier 3 (Professional Negligence). This is mainly because of the rate of reported vulnerabilities and absence of multi-layered security fail-safes, which have indicated a dire need to have standardized frameworks of developer accountability (Roy, 2026; Shapiro, 2025; Ramar et al., 2026).

Discussion: Bridging the "Accountability Vacuum"

The Erosion of Decentralization as a Defense

The empirical results in this paper dismantle the blockchain ethos of Code is Law by showing that autonomous systems do not exist in a legal/social vacuum. The large Gini coefficients in table I and fig. 2 suggests that the majority of the existing DAOs are run as shadow centralized organizations. Legally speaking, such a concentration of power nullifies the defense that no individual is to blame with regard to the consequences of the protocol. A functional fiduciary relationship is created when the top 1% of participants wield most of the votes. This implies that these so-called whales or center developers cannot invoke the defense of decentralization when it has the de facto capability of controlling the direction of the treasury and alter the logic beneath the system.

Benchmarking Professional Negligence

An important contribution of the study is the development of a Foreseeability Index of smart contract vulnerabilities, which offers an objective criterion in assessing diligence of the developers. Professional malpractice can be well determined by the large time difference between the time a bug is reported in security datasets and finally exploited as demonstrated in the absence of some common mitigation techniques, in the case where a reentrancy attack ‘known-bad’ is present in the libraries on which Messi-Q (Messi-Q, https://github.com/Messi-Q/Smart-Contract-Dataset) or SCRUBD Qian et al., (2020) depend, is a breach of the Duty of Care. This empirical norm shifts the focus from the fuzzy law debate around the purpose and intent to a much clearer standard of professional technical care that any software developer dealing with public interest should have.

Risk Distribution and the Role of the Liability Matrix

The Liability Assignment Matrix, fig. 4, suggests that there is a systemic risk within the current ecosystem since the move fast and break things culture of early DeFi is beginning to clash with investor protection. Having 50% of reviewed protocols in Tier 3 (Professional Negligence), it is evident that the roadmap on how to transition these systems into Tier 1 (Safe Harbor) is needed. This can be aided by having a continuous audit of fixed one-time audits and through verified and open-source libraries that are statistically resistant to known exploits of the past. Additionally, it is essential to apply on-chain indicators, indicating power centralization to the participants before investing capital in the institutions to make the institutions remain legitimate.

Aligning Code with Fiduciary Duty

Lastly, fiduciary obligations should not be perceived as hopes in the law but rather as technical limitations in the transition towards strong algorithmic governance. Developers have the ability to demonstrate their compliance with the law by adding the Duty of Loyalty to the deterministic logic of the smart contract, just as it will do with programmed circuit breakers or multi-signature requirements for large treasury movements. This kind of alignment will result in automated governance, ensuring that the fundamental aspects of accountability and stewardship do not become diluted. This cross-functional approach to the problem provides digital jurisprudence with the certainty that the decentralized governance layer will be both innovative and legally compliant, providing further stability to the rapidly evolving fact of digital governance.

V. Conclusion

The evolution of traditional corporate governance to the independent algorithmic systems calls for an urgent and fundamental redefinition of accountability. This study has shown that the so-called Accountability Vacuum of decentralized autonomous organizations (DAOs) is not the technical restriction, but rather the lack of alignment between deterministic code and the legal principles. This paper demonstrated a definite correlation between concentration of power and fiduciary necessity based on empirical evidence synthesized by DeepDAO, Messi-Q, and SCRUBD, as well as an objective "Foreseeability Index" to compare professional developer negligence. The findings suggest that most of the existing protocols are conducted under a shadow centralization that renders the defense of absolute decentralization invalid, and a transition to the suggested Liability Assignment Matrix is needed. Turning to the future, the future development of digital jurisprudence will rely on the effective adoption of the digital jurisprudence concept of Humanistic AI into smart contract logic. Future work ought to focus on creating on-chain fiduciary monitors - automated oracles capable of halting or vetoing governance actions that do not comply with programmed "Duty of Loyalty" parameters. Moreover, since the industry is at the stage of maturity, the introduction of global Technical Standards of Care will be necessary to shift the ecosystem away its current state of ubiquitous professional negligence, towards the state of a safer and more innovative ecosystem exemplified by the state of Safe Harbor. The institutional legitimacy needed to redefine the global financial and legal landscape may be attained by taking fiduciary obligations as technical, as opposed to legal, constraints, and thus changing the next generation of decentralized infrastructure to do so. The resultant product is a harmonious synthesis whereby Code is Law stops being a machine of defense against responsibility, but a machine of programmed trust and integrity of systems.

REFERENCES

[1] Bonnet, S., & Teuteberg, F. (2024). Decentralized autonomous organizations: A systematic literature review and research agenda. *International Journal of Innovation and Technology Management*, *21*(04), 2450026. https://doi.org/10.1142/S0219877024500263

[2] Cesaretti, A. (2025). From Principles to Practice: Measuring the Impact of Governance Reforms in DAOs. In *DAO Governance in Theory and Practice: Metrics, Cases, and Structural Evaluation for Decentralized Autonomous Organizations* (pp. 17-39). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-09675-3_2

[3] De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. *Technology in Society*, *62*, 101284. https://doi.org/10.1016/j.techsoc.2020.101284

[4] Dodig-Crnkovic, G., Basti, G., & Holstein, T. (2025). Delegating responsibilities to intelligent autonomous systems: Challenges and benefits. *Journal of bioethical inquiry*, *22*(3), 507-514. https://doi.org/10.1007/s11673-025-10428-5

[5] Giancaspro, M. (2017). Is a 'smart contract'really a smart idea? Insights from a legal perspective. *Computer law & security review*, *33*(6), 825-835. https://doi.org/10.1016/j.clsr.2017.05.007

[6] Han, J., Lee, J., & Li, T. (2025). A review of DAO governance: Recent literature and emerging trends. *Journal of Corporate Finance*, *91*, 102734. https://doi.org/10.1016/j.jcorpfin.2025.102734

[7] Korytska, O., & Kalmuk, B. (2026). The Paradigm of Decentralized Enterprise Management: A Blockchain-Based Approach. *Stredoevropsky Vestnik Pro Vedu A Vyzkum*, *1*(3). https://doi.org/10.65237/2336-3630-2026-3(1)-2

[8] Luu, L., Chu, D. H., Olickel, H., Saxena, P., & Hobor, A. (2016, October). Making smart contracts smarter. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* (pp. 254-269). https://doi.org/10.1145/2976749.2978309

[9] Mahmoud, A. B., Kumar, V., Berman, A., Elhajjar, S., & Fuxman, L. (2025). Knowledge, attitude and practice towards blockchain potential for digital marketing: scale development and validation. *European Journal of Marketing*, *59*(3), 601-644. https://doi.org/10.1108/EJM-12-2023-0911

[10] Maurya, S., Sato, T., & Hasegawa, M. (2025, October). Advancing DAO Adoption Through Template-driven Design for Applied Governance in Web3. In *2025 7th International Conference on Blockchain Computing and Applications (BCCA)* (pp. 481-488). IEEE. https://doi.org/10.1109/BCCA66705.2025.11229777

[11] Meneguzzo, S., Schifanella, C., Gatteschi, V., & Destefanis, G. (2026, April). Operationalising DAO Sustainability KPIs: A Multi-Chain Dashboard for Governance Analytics. In *Proceedings of the 3rd IEEE/ACM Workshop on Software Engineering Challenges in Financial Firms* (pp. 9-17). https://doi.org/10.1145/3786170.3788388

[12] Messi-Q. *Smart-contract-dataset* [Dataset]. GitHub. https://github.com/Messi-Q/Smart-Contract-Dataset

[13] Qian, P., Liu, Z., He, Q., Zimmermann, R., & Wang, X. (2020). Towards automated reentrancy detection for smart contracts based on sequential models. *IEEE access*, *8*, 19685-19695. https://doi.org/10.1109/ACCESS.2020.2969429

[14] Ramar, K., Ati, M., Hariharan, S., & Kukreja, V. (2026). AI-driven blockchain lending for sustainable development: a machine learning framework for loan risk and eligibility classification. *PeerJ Computer Science*, *12*, e3686. https://doi.org/10.7717/peerj-cs.3686

[15] Roy, A. (2026). Survey of Java Security Practices in Large-Scale Applications. *International Journal of Emerging Research in Engineering and Technology*, *7*(1), 101-108. https://doi.org/10.63282/3050-922x.ijeret-v7i1p115

[16] Schmid, S., & Shestakov, D. (2024, June). Blockchain Governance and Liquid Democracy--Quantifying Decentralization in Gitcoin and Internet Computer. In *Proceedings of the 2024 Workshop on Advanced Tools, Programming Languages, and PLatforms for Implementing and Evaluating algorithms for Distributed systems* (pp. 1-7). https://doi.org/10.1145/3663338.3663678

[17] Shapiro, S. P. (2025). Crypto Fever: Law, Regulation, and the Promise of Trustless Trust. *Annual Review of Law and Social Science*, *21*. https://doi.org/10.1146/annurev-lawsocsci-110124-063008

[18] Steuer, S., & Tröger, T. H. (2022). The role of disclosure in green finance. *Journal of Financial Regulation*, *8*(1), 1-50. https://doi.org/10.1093/jfr/fjac001

[19] Toomey, J. (2025, March 18). *Fiduciary standards* (U Iowa Legal Studies Research Paper No. 2025-17; forthcoming in *ACTEC Law Journal*, Vol. 51, 2026). https://doi.org/10.2139/ssrn.5183968

[20] Wang, S., Ding, W., Li, J., Yuan, Y., Ouyang, L., & Wang, F. Y. (2019). Decentralized autonomous organizations: Concept, model, and applications. *IEEE Transactions on Computational Social Systems*, *6*(5), 870-878. https://doi.org/10.1109/TCSS.2019.2938190

[21] Weidener, L., Bishop-Currey, L., & Fürbeth, M. M. (2025). Organizational Architectures in Biotechnology: Hub-and-Spoke Portfolios and Decentralized Autonomous Organizations. http://dx.doi.org/10.2139/ssrn.5909802