information

MDPI

Article

A Layered Governance Coverage Model for Decentralized Autonomous Organizations: Formalization, Empirical Analysis, and Implications for Blockchain-Based IoT/AI Systems

Abeer S. Al-Humaimeedy [1,*] and Rand Alkharashi [2]

[1] College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[2] Innovative Technologies, Heteen, Riyadh 13518, Saudi Arabia; rand@quintes.org
* Correspondence: abeer@ksu.edu.sa

Abstract

Decentralized Autonomous Organizations (DAOs) enable blockchain-based collective governance, yet existing studies often evaluate DAO governance through isolated mechanisms, particularly voting systems. This narrow view does not sufficiently explain recurring problems such as governance capture, weak accountability, inadequate safeguards, and inefficient resource allocation. This paper proposes a Layered Governance Coverage Model that conceptualizes DAO governance as a system of seven interdependent institutional functions spanning participation, agenda formation, collective choice, safeguards, execution, incentives, and meta-governance. The model uses a four-level strength scale to assess not only whether governance functions are present, but also how strongly they are institutionalized. It is empirically applied to thirty-seven active DAOs through evidence-based coding of publicly available governance artifacts. The results show that governance breadth does not necessarily imply governance maturity: collective choice and execution mechanisms are more developed than accountability, safeguards, and meta-governance. Beyond DAO-native settings, the paper positions governance maturity as a trust and resilience regime for blockchain-based IoT and AI infrastructures, where governance affects security, reliability, data integrity, and risk oversight. The paper discusses AI-enabled governance analytics as a support mechanism for monitoring governance activity, detecting anomalies, and improving governance observability. The proposed framework contributes a structured approach for evaluating and designing resilient governance architectures in DAOs and blockchain-based IoT/AI systems.

Keywords: decentralized autonomous organizations; blockchain-based IoT; artificial intelligence; trust management; security and resilience; data integrity; governance maturity

Check for updates

Academic Editor: Aristeidis Karras

Received: 17 April 2026
Revised: 30 May 2026
Accepted: 3 June 2026
Published: 10 June 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

Decentralized Autonomous Organizations (DAOs) have emerged as a novel organizational form enabled by blockchain and smart contract technologies, facilitating decentralized coordination without centralized managerial authority. DAOs encode governance rules within programmable protocols and rely on collective decision-making processes for proposal submission, voting, resource allocation, and execution [1,2]. In contrast to traditional corporate governance structures, which depend on hierarchical control and legal enforcement mechanisms, DAO governance operates through a combination of algorithmic rule enforcement, tokenized or membership-based participation, and community

coordination [3]. This combination makes DAOs an important socio-technical governance phenomenon rather than merely a technical implementation of voting.

The adoption of DAOs across decentralized finance, public goods funding, protocol governance, ecosystem coordination, and digital communities has intensified scholarly interest in blockchain-based governance systems [4,5]. Prior research emphasizes that governance plays a central role in determining the security, sustainability, legitimacy, and adaptability of decentralized platforms [6]. Core governance dimensions commonly identified include decision rights allocation, accountability mechanisms, incentive alignment, enforcement capacity, and stakeholder participation [7]. Within this broader governance discourse, DAOs represent a particularly complex institutional context because automated execution, economic incentives, and decentralized collective choice must operate together without relying on a conventional managerial hierarchy.

Despite their promise, DAOs continue to experience persistent governance challenges such as power concentration among large token holders, low participation rates, proposal overload, agenda manipulation, weak accountability, and difficulties in monitoring the use of collective resources [4,5,8,9]. These challenges raise fundamental questions regarding the adequacy of existing governance designs and the mechanisms used to evaluate governance effectiveness. In particular, evaluating DAO governance only through isolated mechanisms, such as voting rules or treasury systems, risks overlooking the broader institutional architecture through which participation, proposals, safeguards, execution, incentives, and rule evolution interact.

This problem becomes more significant when blockchain governance is considered in relation to Internet of Things (IoT) infrastructures, edge-enabled services, and data-intensive cyber–physical systems. In such settings, governance does not only affect organizational legitimacy; it may also shape operational trust, security, reliability, resilience, and data integrity. Recent work on blockchain-enabled IoT systems shows that blockchain can strengthen traceability, tamper resistance, auditability, and decentralization, while also introducing governance, scalability, interoperability, and coordination challenges across heterogeneous actors and devices [10]. Related research on decentralized trust management in IoT suggests that secure and reliable operation depends not only on cryptographic mechanisms or distributed ledgers, but also on how authority, validation, intervention, accountability, and adaptation are institutionally organized [11,12]. Accordingly, DAO governance is relevant not only to blockchain-native organizations, but also to emerging blockchain-based IoT and artificial intelligence (AI) enabled infrastructures where governance maturity becomes part of the system's trust and risk-management regime.

This study addresses these challenges by proposing the Governance Coverage Model, a layered institutional framework encompassing the full lifecycle of decentralized collective decision-making. Rather than focusing on isolated governance tools, the model captures the interaction of seven governance functions: participation and legitimacy; agenda control and proposal formation; collective choice mechanisms; accountability and safeguard structures; execution and enforcement; incentive alignment and treasury governance; and operational delegation and meta-governance. The model is designed to evaluate both governance coverage and governance maturity by distinguishing between the mere presence of a governance function and the strength with which that function is institutionalized.

The study makes three main contributions. First, it contributes to DAO governance literature by formalizing a layered model that explains governance robustness as a configuration of interdependent institutional functions rather than as the presence of individual mechanisms. Second, it contributes empirically by applying the model to thirty-seven active DAOs using evidence-based coding of publicly available governance artifacts, thereby producing a comparative governance matrix and descriptive results on layer-wise maturity

and institutional imbalance. Third, it contributes to the broader discussion of blockchain-based IoT and AI systems by interpreting governance maturity as a trust and resilience regime and by outlining how AI-enabled governance analytics may support monitoring, anomaly detection, and risk oversight in decentralized infrastructures.

The practical significance of the model lies in its ability to support governance diagnosis and design. For DAO designers, it identifies where governance systems are institutionally mature and where they remain fragile. For blockchain-based IoT and AI deployments, it provides a structured lens for examining how governance functions influence security, reliability, data integrity, incident response, and adaptive oversight. Accordingly, the paper positions DAO governance not only as a problem of decentralized decision-making, but also as a foundation for trusted and resilient operation in emerging blockchain-enabled digital infrastructures.

2. Literature Review

DAO governance has been increasingly examined as a socio-technical system in which institutional rules are embedded within blockchain protocols and complemented by community-driven coordination processes. Early conceptualizations defined DAOs as blockchain-based self-governing entities capable of automating organizational functions through smart contracts [2]. Subsequent scholarship expanded this view, emphasizing that DAOs represent hybrid institutional arrangements where technical infrastructure, economic incentives, and social dynamics jointly shape governance outcomes [1,13].

Systematic literature reviews on blockchain governance highlight the importance of governance mechanisms in ensuring transparency, accountability, security, and adaptability across decentralized systems [6,7]. These studies identify recurring governance objectives including the allocation of decision rights, enforcement of collective decisions, mitigation of opportunistic behavior, and coordination of diverse stakeholders. Within this governance landscape, DAOs present unique institutional challenges due to open participation, token-based power distribution, and limited reliance on traditional legal enforcement structures.

Empirical analyses demonstrate that DAO governance frequently relies on token-weighted voting systems, often supplemented by delegation mechanisms that allow token holders to assign voting power to representatives or domain experts [4]. While such approaches improve decision efficiency, they also introduce risks of power concentration and governance capture by large token holders. Integrative reviews further reveal that DAO governance structures are shaped by polycentric influences, informal norms, and evolving technical architectures rather than by singular hierarchical control processes [13].

Recent surveys identify a growing diversity of governance mechanisms designed to address DAO coordination challenges, including quadratic voting, reputation-based governance, committee-based decision structures, and hybrid on-chain/off-chain coordination models [5]. However, systematic reviews consistently report persistent governance problems such as Sybil attacks, low voter engagement, agenda manipulation, and weak accountability for treasury expenditures [5,6]. These findings suggest that governance failures often stem from missing or poorly integrated institutional safeguards rather than from deficiencies in individual voting algorithms.

This problem becomes even more significant when blockchain governance interacts with Internet of Things (IoT) infrastructures and data-intensive cyber–physical systems. Recent surveys on blockchain-enabled IoT show that blockchain can strengthen traceability, tamper resistance, auditability, and decentralized trust, while also introducing challenges related to scalability, interoperability, and governance coordination across heterogeneous devices and services [10]. Related research on decentralized trust management in IoT argues that reliable operation depends not only on technical trust mechanisms, but also

on how validation authority, participation, intervention, and adaptation are institutionally organized across the network [11,12]. In such settings, governance is directly linked to operational concerns including security, resilience, service reliability, and data integrity.

A related emerging perspective concerns the role of analytics and artificial intelligence in blockchain-based governance environments. Recent reviews indicate that AI can enhance blockchain systems through anomaly detection, decision support, monitoring, smart-contract analysis, and risk identification [14]. At the same time, computational analysis of DAO ecosystems has shown that governance activity itself can be examined through data-driven techniques, including large-scale trend analysis and governance-pattern interpretation [15]. These developments suggest that DAO governance should be viewed not only as a mechanism for collective decision-making, but also as a potential trust-management and oversight regime for decentralized IoT/AI systems.

From the perspective of blockchain-based IoT and AI systems, this gap is not only conceptual but also operational. IoT infrastructures depend on trusted participation, reliable update procedures, secure data exchange, accountable intervention, and adaptive response to changing technical and organizational conditions. Similarly, AI-enabled decentralized systems require governance arrangements that clarify who may control data flows, modify system parameters, validate outputs, respond to anomalies, and revise oversight rules. Existing blockchain-IoT and AI-blockchain studies provide important insights into security, trust management, anomaly detection, and technical coordination, but they rarely offer an institutional model for evaluating whether the governance architecture itself is sufficiently mature to support security, reliability, data integrity, and resilience. This creates a need for a governance model that can bridge DAO governance research with the trust and risk-management requirements of decentralized IoT/AI infrastructures.

Although existing research provides valuable insights into governance mechanisms and challenges, it exhibits notable limitations. Many studies analyze specific governance tools in isolation, while others propose high-level conceptual frameworks that lack operationalization for empirical evaluation [16]. Moreover, the literature has not sufficiently connected DAO governance maturity to the requirements of blockchain-based IoT/AI deployments, where governance quality may determine whether decentralized infrastructures remain secure, reliable, and adaptable over time. What remains underexplored, therefore, is a comprehensive model capable of integrating governance mechanisms across the entire DAO decision lifecycle while also offering an interpretable basis for analyzing governance robustness in emerging decentralized infrastructures.

In response to this gap, this study introduces the Governance Coverage Model, which conceptualizes DAO governance as a layered system of interdependent institutional functions. By mapping governance mechanisms across participation and legitimacy, agenda control and proposal formation, collective choice mechanisms, accountability and safeguard structures, execution and enforcement, incentive alignment and treasury governance, and operational delegation and meta-governance, the model offers a holistic framework for evaluating governance completeness and vulnerability across diverse DAO systems. Beyond its empirical application to active DAOs, the model also provides a conceptual basis for understanding governance maturity as a trust and resilience regime in blockchain-based IoT/AI environments and for framing AI-enabled governance analytics as a complementary layer of oversight, risk detection, and adaptive support.

3. Governance Coverage Model

This section formalizes the Governance Coverage Model as a layered institutional framework for evaluating DAO governance architectures. The model is derived from governance theory, systematic studies of blockchain governance, and empirical evidence

on DAO coordination failures. Rather than treating governance as a set of isolated tools (e.g., voting mechanisms), the model conceptualizes governance as an interdependent institutional system whose effectiveness depends on both the scope of governance functions covered and the strength with which those functions are institutionalized. This framing responds directly to the limitation identified in the literature review: existing work has generated important insights into specific DAO governance mechanisms and risks, but it has not sufficiently operationalized governance as a lifecycle-spanning institutional architecture that can be compared systematically across DAOs and interpreted in broader decentralized infrastructures.

3.1. Derivation of the Layered Governance Architecture

Prior research on blockchain and DAO governance consistently emphasizes that governance outcomes are shaped by multiple interacting institutional mechanisms rather than by voting procedures alone. Systematic reviews identify decision rights allocation, accountability structures, incentive alignment, and enforcement capacity as recurring governance dimensions across decentralized systems [6,7]. Integrative studies further show that DAO governance is a socio-technical phenomenon in which technical protocols, economic incentives, and social coordination jointly shape governance effectiveness [1,13].

Empirical surveys and reviews of DAO governance mechanisms report substantial heterogeneity in the design of proposal pipelines, voting schemes, delegation structures, treasury governance, and safeguards [4,5]. These differences are not merely cosmetic: empirical work documents that tokenized governance often concentrates power among large holders and may be weakly exercised in practice despite nominal openness [8,9]. Complementary evidence also indicates that off-chain voting can reduce participation frictions while altering transparency and enforceability properties, with measurable implications for DAO outcomes [17,18]. Together, these findings motivate a governance model that captures governance as a lifecycle-spanning architecture rather than a single mechanism.

Existing governance frameworks commonly analyze governance mechanisms in isolation or provide high-level conceptual descriptions without an operational structure suitable for comparative evaluation [16]. In response, we conceptualize DAO governance as a layered architecture comprising seven interdependent governance functions. The model is intentionally function-centered rather than tool-centered: it asks what institutional work a governance system must perform, not merely which governance technologies it visibly adopts.

The selection of the seven governance functions followed four design criteria. First, each function had to recur in the reviewed literature as a distinct governance concern rather than as a one-off implementation detail. Second, the set had to provide lifecycle completeness, covering the institutional sequence from participation and authority, through proposal formation and decision-making, to enforcement, economic alignment, and adaptation. Third, each function had to be empirically observable through public governance artifacts, enabling evidence-based coding across heterogeneous DAOs. Fourth, the set had to preserve analytical separability, meaning that the layers are conceptually distinguishable even when implemented through the same technical platform or governance interface.

This function-first specification also clarifies the boundaries of the model. Several plausible candidates, including transparency, decentralization, trust, inclusiveness, legitimacy, and security, were considered during model derivation but were not retained as separate layers because they operate more appropriately as cross-cutting properties, evaluation criteria, or outcomes that emerge from the interaction of multiple governance functions. For example, legitimacy is shaped by participation, agenda control, and collective choice; trust depends on participation, safeguards, enforcement, and incentives; and decentraliza-

tion is distributed across several layers rather than contained within a single governance function. Similarly, technical components such as network infrastructure, data storage, and application services were excluded because the present model is scoped specifically to governance architecture rather than the full technical stack of decentralized systems.

Accordingly, we conceptualize DAO governance as a layered architecture comprising the following seven interdependent governance functions:

- **Participation and legitimacy**: mechanisms defining eligibility for governance participation, membership or stake-based decision rights, and the basis of governance authority, including the distribution and exercise of voting rights [9,18];
- **Agenda control and proposal formation**: institutional processes regulating who may initiate proposals, how proposals are structured and filtered, and how agenda-setting power is constrained throughout the proposal lifecycle [18,19];
- **Collective choice mechanisms**: preference aggregation procedures including token-weighted voting, delegation, and alternative mechanisms such as quadratic voting, together with quorum and threshold rules [8,20,21];
- **Accountability and safeguard structures**: institutional constraints designed to mitigate governance risks, including dispute resolution, emergency interventions, cancellation rights, risk controls, and role- or identity-aware governance elements [8,9,19];
- **Execution and enforcement processes**: mechanisms that translate approved decisions into binding actions via on-chain execution, timelocks, controlled executors, or hybrid on-/off-chain enforcement [17,19];
- **Incentive alignment and treasury governance**: economic mechanisms governing reward distribution, funding allocation, and financial accountability, including incentive channels that may introduce capture or bribery dynamics [9,22,23];
- **Operational delegation and meta-governance**: structures enabling delegation of authority to specialized roles, committees, or sub-DAOs, and mechanisms for modifying governance rules and institutional parameters over time [8,18,19].

These layers reflect the sequential and complementary nature of governance processes observed across decentralized systems and provide a structured basis for evaluating institutional completeness. Collectively, they cover entry, initiation, decision, constraint, enactment, economic alignment, and institutional adaptation. The analytical purpose of the model is therefore not to claim that all DAOs must instantiate identical governance forms, but to provide a common institutional vocabulary through which governance architectures can be compared, interpreted, and evaluated.

3.2. Layer Strength Scoring Scheme

A binary notion of governance coverage (present vs. absent) is insufficient for empirical comparison because DAOs often implement the same governance layer with markedly different degrees of enforceability, decentralization, and robustness. Empirical evidence shows that tokenized governance can be highly concentrated and only weakly exercised in practice, despite nominally open participation rights, indicating that the existence of a layer does not imply that the layer functions effectively [8,9]. Evidence on off-chain voting further suggests that governance mechanisms can trade off scalability and accessibility against bindingness and transparency, affecting governance outcomes and value creation [17,18]. Therefore, we introduce a layer strength scale that evaluates each layer not only by existence but by the quality of institutionalization.

Across all layers, we operationalize strength using a four-level ordinal scale:

- **0 = Not available**: no public evidence of a mechanism or the DAO does not expose the relevant governance interface/data.

- **1 = Weak**: mechanism exists informally or off-chain without binding effect; rules are discretionary or sparsely used.
- **2 = Moderate**: mechanism is defined and regularly used, but enforcement is partial, data are incomplete, or known vulnerabilities remain material.
- **3 = Strong**: mechanism is explicit, consistently used, auditable, and includes safeguards against major threats relevant to the layer.

The scale is intentionally conservative: scores above 1 require auditable evidence of repeated use, and scores of 3 require both institutional clarity and threat-aware design consistent with known empirical failure modes (e.g., concentration, collusion, low participation, bribery markets) [8,21,22].

For **L1 (Participation and Legitimacy)**, strength can be operationalized via participation rates and engagement concentration in governance processes, particularly in off-chain voting environments [18]. Political-economy analyses emphasize that tradability of voting power can structurally bias participation toward elites, producing timocratic governance even under nominally open participation rules [9]. Empirical evidence also suggests that governance configurations diverging from on-chain enforceability ideals, including reliance on off-chain coordination, can be associated with measurable differences in value creation and governance effectiveness [17]. Accordingly, score 1 reflects ad hoc inclusion without measurable engagement; score 2 requires repeated evidence of participation processes; and score 3 requires auditable inclusion with mitigations against concentration and exclusion [8,9].

For **L2 (Agenda Control and Proposal Formation)**, policy-based governance frameworks treat proposal lifecycle rules as formal policy objects governing admissibility, roles, and activation, thereby increasing clarity and auditability [19]. However, empirical analyses of large-scale voting environments show that proposal production and attention can be highly skewed, implying concentration of agenda-setting power even in open systems [18]. Strength therefore depends on both formal process design and credible constraints against agenda capture: score 1 corresponds to unclear or discretionary proposal rules; score 2 reflects explicit pipelines with repeated usage; and score 3 requires auditable lifecycle rules and mechanisms that limit unilateral agenda control [18,19].

For **L3 (Collective Choice Mechanisms)**, mechanism-design research evaluates alternative aggregation schemes such as quadratic voting and analyzes their incentive compatibility in decentralized settings [20]. Adversarial robustness studies emphasize whale dominance and collusion vulnerabilities and propose voting mechanisms designed to resist these threats [21]. Empirical analysis of delegation structures further shows that delegation can reshape effective control and must be evaluated through observed voting power dynamics rather than inferred from formal rules [8]. Accordingly, strength is anchored by robustness to concentration and collusion: score 1 indicates basic voting with limited safeguards; score 2 indicates documented mechanisms with repeated usage; and score 3 requires explicit defenses against whale/collusion dynamics and evidence that the mechanism operates as intended [8,20,21].

For **L4 (Accountability and Safeguards)**, identity- and role-aware governance frameworks propose enhancing fairness, security, and directed participation through policy-based on-chain governance and role constraints [19]. Empirical risk framing indicates that concentrated tokenized voting rights and low exercise can undermine accountability unless complemented by explicit safeguards [8,9]. Strength therefore depends on auditable safeguard design and credible intervention conditions: score 1 reflects informal social accountability only; score 2 requires explicit safeguards with documented invocation conditions; and score 3 requires safeguards that are auditable and threat-linked to empirically observed failure modes such as elite capture and collusion [8,9].

For **L5 (Execution and Enforcement)**, the distinction between on-chain and off-chain governance is empirically consequential. Off-chain voting can reduce cost and complexity but may reduce transparency and bindingness, with documented implications for governance effectiveness and value outcomes [17]. Policy-based on-chain governance architectures encode proposal activation and execution rules, thereby improving enforceability and auditability [19]. Strength thus reflects bindingness: score 1 corresponds to non-binding outcomes; score 2 corresponds to partially binding hybrid execution; and score 3 requires binding execution with auditable enforcement and a clear linkage between vote outcome and action [17,19].

For **L6 (Incentive Alignment and Treasury Governance)**, governance incentives can create both efficiency and vulnerability. Bribe-market analyses show that governance ecosystems can evolve competitive markets for voting power, steering outcomes toward payers rather than collective welfare [22]. Public goods funding studies highlight that quadratic funding can improve allocation but remains strategically vulnerable under matching-fund constraints [23]. Political-economy framing emphasizes that tradable voting rights can structurally bias governance toward wealth-weighted outcomes [9]. Strength therefore reflects the economic integrity of governance: score 1 reflects implicit incentives only; score 2 reflects explicit incentive rules with observable treasury processes; and score 3 requires evidence of anti-capture design consistent with known incentive pathologies such as bribery markets and wealth-based control [9,22].

For **L7 (Operational Delegation and Meta-Governance)**, empirical work demonstrates that formal decentralization can differ from effective control, and delegation must therefore be assessed via observed delegate networks and voting behavior [8]. Governance-as-policy modularity supports iterative change, role separation, and auditable evolution of governance rules [19]. Evidence from large DAO populations suggests that governance structures co-evolve with platform constraints and community engagement patterns [18]. Strength thus reflects accountable delegation and institutional adaptability: score 1 indicates informal delegation without accountability; score 2 indicates documented delegation structures; and score 3 requires auditable delegation and mechanisms supporting transparent and safe rule evolution [8,19].

Implication for the Coverage Matrix

The strength scale converts the Governance Coverage Model into an analyzable instrument in which each DAO is represented as a vector of layer-strength scores. This enables comparative evaluation of governance maturity across DAO categories, identification of systematic weaknesses (e.g., strong voting but weak safeguards), and statistical analysis linking governance strength to observable outcomes where data are available.

3.3. Formal Definition of Strength-Aware Governance Coverage

Let a DAO governance system be represented as a set of governance mechanisms:

$$G = \{g_1, g_2, \ldots, g_n\}, \tag{1}$$

where each g_j denotes a governance mechanism used to implement decision-making, coordination, control, or enforcement processes. We define the Governance Coverage Model as a mapping of these mechanisms onto a predefined set of governance layers:

$$L = \{L_1, L_2, \ldots, L_7\}, \tag{2}$$

where each layer corresponds to a core institutional governance function. For a given DAO d, governance coverage is represented by a strength vector:

$$C_d = (s_{d1}, s_{d2}, \ldots, s_{d7}), \tag{3}$$

where s_{di} indicates the institutional strength of layer L_i for DAO d, with:

$$s_{di} \in \{0, 1, 2, 3\}. \tag{4}$$

We interpret s_{di} according to the four-level ordinal scale defined above, where 0 indicates no explicit evidence of the layer and 3 indicates strong, auditable, threat-aware institutionalization.

Each layer corresponds to the following institutional function:

- L_1 (Participation and Legitimacy): eligibility, distribution of decision rights, and participation conditions [9,18];
- L_2 (Agenda Control and Proposal Formation): proposal initiation, filtering, and lifecycle governance [18,19];
- L_3 (Collective Choice Mechanisms): voting, delegation, and aggregation robustness [8,20,21];
- L_4 (Accountability and Safeguards): dispute resolution and institutional constraints against harmful actions [9,19];
- L_5 (Execution and Enforcement): binding implementation of decisions via on-chain or hybrid enforcement [17,19];
- L_6 (Incentive Alignment and Treasury Governance): incentive design and treasury integrity under adversarial economic pressures [9,22,23];
- L_7 (Operational Delegation and Meta-Governance): delegation structures and rule-evolution capacity [8,18,19].

Governance maturity for DAO d can be expressed as an aggregate strength index:

$$\Gamma_d = \sum_{i=1}^{7} s_{di}, \tag{5}$$

where higher values indicate broader and stronger institutional governance coverage.

The use of an unweighted sum is intentional. In this study, the aggregate maturity index is used as a descriptive baseline measure rather than as a claim that all layers are equally consequential in every deployment context. An unweighted formulation preserves transparency, avoids imposing contestable prior assumptions about the relative importance of the seven layers, and supports straightforward comparison across heterogeneous DAOs. Accordingly, Γ_d should be interpreted as a parsimonious summary of the breadth and strength of governance institutionalization, not as a complete risk-weighted measure of governance quality.

At the same time, the model does not assume that all layers have equal operational consequences under all conditions. In blockchain-based IoT and AI deployments, certain layers may function as high-criticality or gatekeeper layers. In particular, weak accountability and safeguards (L_4) or weak execution and enforcement (L_5) may undermine trust, security, and resilience even when other governance layers are moderately mature. Future work may therefore extend the present descriptive index through weighted, non-compensatory, or domain-specific variants in which selected layers receive greater importance under safety-critical or infrastructure-oriented conditions.

This formulation supports systematic comparison of DAO governance architectures by evaluating governance robustness as an emergent institutional property shaped by interact-

ing governance layers and their maturity, rather than by the presence of isolated governance mechanisms. It also preserves analytical flexibility: the same formal representation can support future weighted variants, threshold-based variants, or domain-specific adaptations without changing the underlying governance architecture specified by the model.

4. Empirical Application of the Governance Coverage Model to Active DAOs

This section operationalizes the Governance Coverage Model and applies it to a dataset of thirty-seven active DAOs. The empirical objective is twofold: (i) to construct a reproducible governance representation capturing both coverage and strength for each DAO across the seven layers, and (ii) to analyze cross-DAO patterns of institutional maturity prior to interpreting broader governance implications. In contrast to binary presence/absence coding, the empirical protocol follows the four-level strength scale defined in Section 3, enabling comparability across DAOs that implement the same layer with different degrees of enforceability, decentralization, and robustness [8,9,17].

4.1. DAO Dataset and Scope

The empirical dataset comprises thirty-seven DAOs selected to reflect diversity in governance purpose and institutional design. The sample covers (i) protocol and treasury governance DAOs, (ii) organizational and guild DAOs, (iii) public goods and funding DAOs, (iv) infrastructure and ecosystem governance DAOs, (v) dispute and safeguard DAOs, and (vi) impact and specialized DAOs. This categorization is consistent with governance typologies reported in DAO governance surveys and reviews [4,5].

DAOs were included if they exhibited (a) observable governance activity (e.g., proposal lifecycle, voting, treasury allocation) and (b) publicly available governance documentation sufficient for evidence-based coding. This inclusion logic reflects best practices in blockchain governance empirical studies that prioritize verifiable governance artifacts over informal community narratives [6,7].

The sample should therefore be interpreted as a purposive, evidence-oriented sample rather than as a statistically representative sample of all DAOs. The objective was not to estimate the population distribution of DAO governance forms, but to evaluate whether the Governance Coverage Model can be operationalized across diverse and sufficiently documented DAO settings. DAOs with minimal public governance activity, inactive proposal records, inaccessible governance documentation, or insufficiently traceable governance artifacts were excluded because they could not support reliable layer-level coding. This selection strategy improves auditability and reproducibility, but it may also bias the sample toward DAOs that maintain more formal and publicly visible governance infrastructures.

4.2. Data Sources and Collection Protocol

Governance evidence was collected exclusively from publicly available and verifiable sources. Primary sources included official DAO governance documentation (e.g., protocol governance specifications, governance portals), repositories containing formal governance rules or parameters, and official governance discussion forums where proposal lifecycles and operational policies are documented. Secondary sources were used only to support triangulation and contextual interpretation when consistent with primary records [5,6].

Because DAO governance frequently spans on-chain execution and off-chain coordination, the collection protocol explicitly captured both:

- **On-chain governance artifacts**: execution contracts (e.g., timelocks), on-chain proposal parameters (quorum, thresholds), and auditable treasury transactions where applicable [19].

- **Off-chain governance artifacts**: Snapshot voting records, proposal repositories, and publicly maintained governance dashboards, recognizing that off-chain voting can alter transparency and enforceability properties [17,18].

All coded claims were supported by at least one traceable artifact. When governance information for a layer could not be verified, that layer was coded as not available (score 0), rather than inferred.

The full list of DAOs, their category assignments, and their primary governance evidence is provided in Table 1.

Table 1. Active DAOs included in the empirical analysis, governance category, and primary governance evidence.

DAO Name	Governance Category	Primary Governance Evidence
Aave DAO	Protocol & Treasury Governance	Governance documentation; on-chain Governor; Snapshot [24]
Compound DAO	Protocol & Treasury Governance	On-chain Governor; proposal archive [25]
MakerDAO	Protocol & Treasury Governance	Governance portal; forums; executive votes [26]
Curve DAO	Protocol & Treasury Governance	Snapshot; on-chain gauges; governance documentation [27]
Element Finance DAO	Protocol Governance	Governance documentation; Snapshot [28]
Babylon DAO	Protocol Governance	Governance forum; proposal records [29]
Inverse Finance DAO	Protocol & Treasury Governance	Governance documentation; Snapshot [30]
Ooki DAO	Protocol Governance	Governance contracts; proposal records [31]
mStable DAO	Protocol Governance	Governance documentation; Snapshot [32]
UXD Protocol DAO	Protocol Governance	Governance documentation; governance token UXP documentation [33]
dxDAO	Organizational/Guild DAO	DAOstack governance framework; forums [34]
Moloch DAO	Organizational/Guild DAO	Moloch framework documentation; proposals [35]
LexDAO	Organizational/Guild DAO	Governance forum; proposal records [36]
RaidGuild DAO	Organizational/Guild DAO	Governance documentation; Snapshot [37]
1Hive DAO	Organizational/Guild DAO	Governance portal; proposal lifecycle records [38]
PrimeDAO	Organizational/Guild DAO	Governance documentation; Snapshot [39]
Yam DAO/Yam House	Organizational DAO	Governance documentation; proposal archive [40]
Gitcoin DAO	Public Goods & Funding DAO	Governance portal; grants rounds documentation [41]
Mango DAO	Public Goods/Protocol DAO	Governance forum; Snapshot [42]
Ocean DAO	Public Goods & Ecosystem DAO	Governance documentation; Snapshot [43]
Polygon Grants DAO	Public Goods & Funding DAO	Grants governance documentation [44]
Commons Stack DAO	Public Goods DAO	Governance framework; proposal records [45]
Panvala DAO	Public Goods DAO	Funding governance documentation [46]
People DAO	Public Goods/Social DAO	Governance forum; Snapshot [47]
PoolTogether DAO	Protocol/Public Goods DAO	Governance portal; proposal archive [48]
Decentraland DAO	Metaverse/Public DAO	Governance portal; voting records [49]
Cardano Project Catalyst	Infrastructure Governance	Catalyst governance documentation; voting platform [50]
Dash DAO	Infrastructure Governance	Treasury governance documentation [51]
Polkadot Governance	Infrastructure Governance	On-chain governance; referenda records [52]
Kusama Governance	Infrastructure Governance	On-chain governance; referenda records [53]
Moonbeam DAO	Infrastructure/Protocol DAO	Governance documentation [54]
Kleros DAO	Dispute & Safeguard DAO	Arbitration and governance documentation [55]
MiraDAO	Specialized DAO	Governance documentation [56]
RVRS DAO	Impact/Climate DAO	Governance forum; proposal archive [57]
Cosmos Hub Governance	Infrastructure Governance	On-chain governance; proposal archive [58]
IOTA Governance	Infrastructure Governance	Governance framework documentation [59]
Nexus Mutual DAO	Risk/Insurance DAO	Governance documentation; voting records [60]

4.3. Coding Scheme: Layer Strength Assessment

Each DAO d was coded on each governance layer L_i using the four-level ordinal strength scale defined in Section 3. The resulting governance representation is the strength vector defined in Equation (3), with the score domain specified in Equation (4).

Coding followed a function-first principle: evidence was mapped to a layer based on the institutional function it performs, not the platform that hosts it. For example, a proposal pipeline implemented via a forum policy and Snapshot vote was coded under agenda control and collective choice, whereas binding on-chain timelock execution was coded under execution and enforcement [17,19].

To reduce ambiguity in the ordinal scale, we applied operational anchors informed by known governance threats:

- **Strength 1 (Weak)** indicates informal, discretionary, or sparsely used mechanisms without clear enforceability.
- **Strength 2 (Moderate)** indicates formally defined mechanisms that are used in practice but retain material vulnerabilities or partial enforcement.
- **Strength 3 (Strong)** requires auditable enforcement and explicit threat-aware design targeting empirically documented failure modes such as concentration, collusion, and bribery markets [8,21,22].

The full scoring rubric used in the empirical analysis is provided in Appendix A.

Layer-specific interpretation followed the conceptual anchors in Section 3. For example, L1 strength considered both participation and distribution of decision rights, reflecting evidence that governance can be nominally open yet effectively timocratic [9]. L3 strength considered robustness to whale dominance and collusion, consistent with mechanism-design and adversarial voting literature [20,21]. L6 strength considered incentive integrity under vote-buying and cross-protocol bribery dynamics [22].

4.4. Evidence Rules, Non-Inference Policy, and Documentation Bias

To preserve empirical rigor and avoid over-estimating governance maturity, the following evidence rules were enforced:

- **Explicitness**: A layer received a non-zero score only when its mechanisms were explicitly described in a primary governance artifact or in a source that directly cites the governing rules.
- **Auditability**: Scores above 1 required evidence of repeated operational use or auditable enforcement (e.g., executed proposals, recurring grants cycles, or documented invocation conditions for safeguards).
- **Threat-aware justification**: A score of 3 required evidence that the mechanism is designed to mitigate a relevant governance threat (e.g., whale dominance, collusion, bribery markets, agenda capture), consistent with the scale definition [8,21,22].
- **No inference**: If documentation was incomplete, ambiguous, or inconsistent, the layer was coded as 0 (not available) or 1 (weak), and the limitation was recorded.

This conservative non-inference policy is aligned with the methodological stance in blockchain governance reviews that emphasize traceable governance evidence [6,7].

At the same time, this evidence strategy introduces a potential documentation bias. Because scoring relies on publicly available and traceable governance artifacts, DAOs with sophisticated but informal, socially embedded, or weakly documented governance practices may receive lower scores than their actual institutional practice would suggest. This limitation is particularly relevant for DAOs whose governance occurs through informal deliberation, private coordination channels, community norms, or ad hoc working groups that are not consistently archived in public governance records. Therefore, a low score

should be interpreted as a lack of publicly verifiable governance maturity rather than definitive proof that the corresponding institutional function is entirely absent. The conservative scoring policy strengthens empirical reproducibility, but it may understate governance maturity in DAOs where governance is real but less formally documented.

4.5. Reliability, Triangulation, and Validation

DAO governance evidence is distributed across heterogeneous platforms and may evolve rapidly. To address reliability risks, we applied a triangulation protocol: whenever possible, each coded mechanism was validated using multiple artifacts (e.g., governance documentation plus executed proposal records; forum policy plus voting archive). When discrepancies were observed, primary governance documentation and on-chain artifacts were prioritized over interpretive summaries [6].

To support reproducibility, we maintained a coding log linking each layer score to its supporting artifacts, including source type (on-chain/off-chain), publication date, and the specific governance component referenced. This approach mitigates common empirical threats in DAO studies, such as incomplete visibility of off-chain coordination, inconsistent terminology across DAOs, and non-equivalence of governance platforms [8,18].

4.6. Pre-Results Outputs: Coverage Matrix Construction

The coding protocol produces a governance coverage matrix $M \in \mathbb{Z}^{37\times 7}$, where $M_{d,i} = s_{di}$ represents the strength of layer L_i for DAO d. This matrix operationalizes the Governance Coverage Model as a comparative instrument, enabling both descriptive and statistical analysis of institutional maturity across DAO categories. The matrix also supports identification of systematic governance gaps, such as DAOs with strong collective choice mechanisms but weak accountability or enforcement structures, which prior work suggests can lead to governance failure despite active voting [9,17].

4.7. Results Overview

The following subsections report descriptive statistics and comparative analyses derived from the coverage matrix, including layer-wise strength distributions, governance maturity profiles by DAO category, and cross-layer institutional imbalances. The analysis remains descriptive and cross-sectional. It identifies layer-wise maturity patterns, category-level differences, and cross-layer imbalances, but does not claim causal relationships between governance maturity and downstream outcomes without longitudinal or experimental identification.

4.7.1. Governance Breadth Versus Governance Strength

The empirical application of the Governance Coverage Model shows that governance breadth and governance maturity are analytically distinct. Many DAOs in the sample exhibit broad formal governance coverage in the sense that multiple governance layers are visibly present. However, once those layers are evaluated using the four-level strength scale, substantial variation emerges in the quality, enforceability, and robustness of implementation. In other words, the presence of a governance layer does not by itself imply that the corresponding institutional function is strongly developed.

This distinction is important because binary governance presence tends to overestimate institutional maturity in environments where governance mechanisms are visible but weakly enforced or weakly exercised in practice. The empirical results therefore support the need for a strength-aware model rather than a purely presence-based governance taxonomy, consistent with prior DAO governance research showing that formal participation and voting rights may coexist with concentrated control and weak practical accountability [8,9].

4.7.2. Layer-Level Governance Maturity

The layer-wise analysis reveals that governance maturity is unevenly distributed across the seven institutional layers. Collective choice mechanisms (L3) and agenda control (L2) are among the most consistently developed layers across the sample, reflecting the widespread adoption of proposal pipelines, voting procedures, and quorum-based decision processes. Participation and legitimacy (L1) is also widely present, but its strength is often limited by concentration of governance power and uneven participation.

By contrast, accountability and safeguards (L4) emerge as the least mature layer across the sample. Although some DAOs implement veto rights, emergency controls, or challenge procedures, these mechanisms are often absent, weakly specified, or limited in scope. Operational delegation and meta-governance (L7) also remain comparatively underdeveloped, indicating that many DAOs are more capable of making and executing decisions than of systematically evolving their own governance structures over time.

Execution and enforcement (L5) tends to be more mature in technically oriented DAOs, particularly where governance outcomes are linked to on-chain execution, timelocks, or other auditable mechanisms. Incentive alignment and treasury governance (L6) is widely present due to the prominence of grants, contributor compensation, and treasury allocation in many DAO systems, although its robustness varies substantially depending on resistance to manipulation and concentration. Overall, these results indicate that technical decision layers generally mature faster than social-institutional constraint layers, which is consistent with prior work on uneven institutionalization in DAO governance [8,17,21].

4.7.3. Governance Maturity Across DAO Categories

To examine whether governance maturity varies systematically with DAO function, the thirty-seven DAOs were grouped into four broader governance families: protocol-oriented, infrastructure-oriented, organizational and guild-oriented, and mission- and funding-oriented DAOs. This grouping aggregates the more specific categories reported in Table 1 into analytically meaningful families while avoiding excessive fragmentation into very small subgroups.

For each DAO, category-level comparison was based on the aggregate governance maturity index defined in Equation (5), which summarizes the breadth and strength of governance institutionalization across all seven layers. Table 2 reports the resulting descriptive statistics by DAO family.

Table 2. Aggregate governance maturity by broader DAO family. The table summarizes the governance maturity index Γ_d across grouped DAO categories.

DAO Family	Count	Mean Γ_d	Median	Min	Max
Protocol-oriented	13	11.77	12.00	5	18
Infrastructure-oriented	7	11.57	12.00	6	17
Organizational and guild-oriented	8	9.38	10.50	2	13
Mission- and funding-oriented	9	8.67	8.00	5	18

Table 2 shows that protocol-oriented DAOs exhibit the highest average governance maturity, followed closely by infrastructure-oriented DAOs. This result is consistent with the institutional demands of protocol maintenance, parameter governance, and binding execution, all of which require relatively mature collective choice and enforcement mechanisms. Infrastructure-oriented DAOs display a similarly high maturity profile, reflecting their dependence on formal governance procedures for ecosystem coordination, referenda, and protocol-level upgrades.

By contrast, organizational and guild-oriented DAOs display lower aggregate maturity, despite often having visible coordination structures and community processes. This suggests that operational coordination alone does not necessarily produce strong institutionalization across all governance layers, particularly where safeguards, execution, and meta-governance remain weakly formalized. Mission- and funding-oriented DAOs exhibit the lowest average maturity score, although the category also shows substantial internal variation. These differences indicate that governance maturity is partly shaped by DAO function, but structural weaknesses—particularly in safeguards and legitimacy—persist across categories, consistent with prior observations in DAO governance studies [8,9,21].

These category-level differences should also be interpreted in light of documentation visibility. Protocol- and infrastructure-oriented DAOs often rely on on-chain execution, formal parameter governance, public proposal archives, and technical governance documentation. These artifacts are comparatively easier to observe and code. By contrast, organizational, guild-oriented, mission-oriented, and funding-oriented DAOs may rely more heavily on social norms, informal deliberation, community moderation, or discretionary working-group practices. Such practices may perform genuine governance functions while leaving fewer publicly auditable traces. Consequently, part of the maturity gap between protocol/infrastructure DAOs and mission/funding DAOs may reflect a visibility asymmetry in governance documentation, not only a substantive difference in institutional quality. The results should therefore be read as comparative evidence of publicly verifiable governance maturity, rather than as a complete ranking of all formal and informal governance capacity.

4.7.4. Cross-Layer Patterns and Institutional Imbalances

The completed governance matrix reveals recurring cross-layer imbalances across the sample. The most persistent pattern is the asymmetry between decision capacity and institutional constraint. Many DAOs exhibit relatively mature agenda control, voting, and execution layers while showing weaker accountability and safeguard mechanisms. In practical terms, this means that governance systems may be relatively capable of making and enacting decisions without being equally capable of contesting, constraining, or reversing harmful decisions.

A second recurring pattern is the decoupling of formal participation from effective control. In several DAOs, participation mechanisms are nominally open, yet governance authority remains substantively concentrated. This pattern aligns with prior empirical findings showing that formal decentralization may coexist with concentrated exercise of power in token-based governance systems [8,9].

A third pattern concerns the asymmetry between treasury governance and institutional oversight. In a number of DAOs, treasury allocation and incentive systems are more developed than the accountability mechanisms capable of constraining strategic or manipulative funding behavior. This imbalance is especially important in mission- and funding-oriented DAOs, where resource allocation is a central governance task but may be exposed to capture, strategic grant-seeking, or weak auditability [22,23].

4.7.5. Quantitative Summary of Governance Maturity

To complement the qualitative interpretation, descriptive statistics were computed directly from the completed DAO-by-layer governance matrix. For each DAO d, governance maturity is represented by the seven-dimensional strength vector defined in Equation (3), with each layer score following the domain specified in Equation (4).

The scores were assigned using the coding and evidence rules described in Sections 4.3 and 4.4, based exclusively on publicly documented governance artifacts drawn from official

governance portals, proposal archives, voting interfaces, and auditable governance records for the thirty-seven DAOs listed in Table 1. This approach follows established empirical practice in blockchain governance research, which prioritizes traceable governance evidence over informal or undocumented claims [6,7].

Layer-level descriptive statistics were calculated from the completed matrix. For each governance layer L_i, the mean strength score was computed as:

$$\bar{s}_i = \frac{1}{N} \sum_{d=1}^{N} s_{di}, \tag{6}$$

where $N = 37$ is the number of DAOs in the sample. To identify the extent of highly mature implementation, the percentage of DAOs receiving the maximum score ($s_{di} = 3$) was computed as:

$$P_i^{\text{strong}} = \frac{|\{d : s_{di} = 3\}|}{N} \times 100, \tag{7}$$

where P_i^{strong} denotes the percentage of DAOs with strong implementation in layer L_i.

At the DAO level, overall governance maturity was summarized using the aggregate governance maturity index defined in Equation (5), which captures the breadth and strength of institutionalization across all governance layers.

Across the sample, the mean DAO-level maturity score is 10.46 out of a maximum possible 21, with a median of 11, an interquartile range of 7–13, a minimum of 2, and a maximum of 18. These values indicate that the sample is neither institutionally minimal nor uniformly mature; rather, most DAOs occupy a middle range characterized by uneven development across layers.

Table 3 reports the layer-level quantitative results. Collective choice mechanisms (L3) display the highest mean strength score (2.08), followed by agenda control and proposal formation (L2) at 1.78 and participation and legitimacy (L1) at 1.73. By contrast, accountability and safeguards (L4) exhibit the lowest mean score (0.89), followed by operational delegation and meta-governance (L7) at 1.03. These results quantitatively reinforce the central empirical claim of the Governance Coverage Model: governance coverage does not imply governance maturity. Many DAOs implement core governance layers in form, but comparatively fewer institutionalize them at a high level of robustness, consistent with prior findings on voting concentration, governance fragility, and uneven institutionalization in DAO governance [8,9,21].

Table 3 shows that the strongest layers in the current DAO landscape are those most directly tied to operational decision-making, namely collective choice and agenda control, whereas the weakest layers are those associated with institutional constraint and structured governance evolution. This imbalance suggests that many DAOs have developed the capacity to initiate, decide, and execute governance actions without equivalently mature mechanisms for constraining harmful outcomes or adapting governance structures over time.

Figure 1 provides a visual representation of the completed DAO-by-layer governance matrix. Each row corresponds to one DAO and each column corresponds to one governance layer, with color intensity reflecting the assigned strength score on the 0–3 scale. The figure complements Table 3 by showing not only average layer maturity, but also the distribution of governance strength across individual DAOs. This makes visible both category-level clustering and recurrent structural imbalances across the sample.

Table 3. Layer-wise governance maturity across the 37-DAO sample. Mean and median are calculated on the 0–3 layer-strength scale. Strong Impl. (%) refers to the percentage of DAOs receiving a score of 3 in the corresponding layer.

Governance Layer	Mean	Median	Strong Impl. (%)
L1 Participation and Legitimacy	1.73	2.00	2.7
L2 Agenda Control and Proposal Formation	1.78	2.00	16.2
L3 Collective Choice Mechanisms	2.08	2.00	29.7
L4 Accountability and Safeguards	0.89	1.00	2.7
L5 Execution and Enforcement	1.51	1.00	13.5
L6 Incentive Alignment and Treasury Governance	1.43	2.00	8.1
L7 Operational Delegation and Meta-Governance	1.03	1.00	10.8

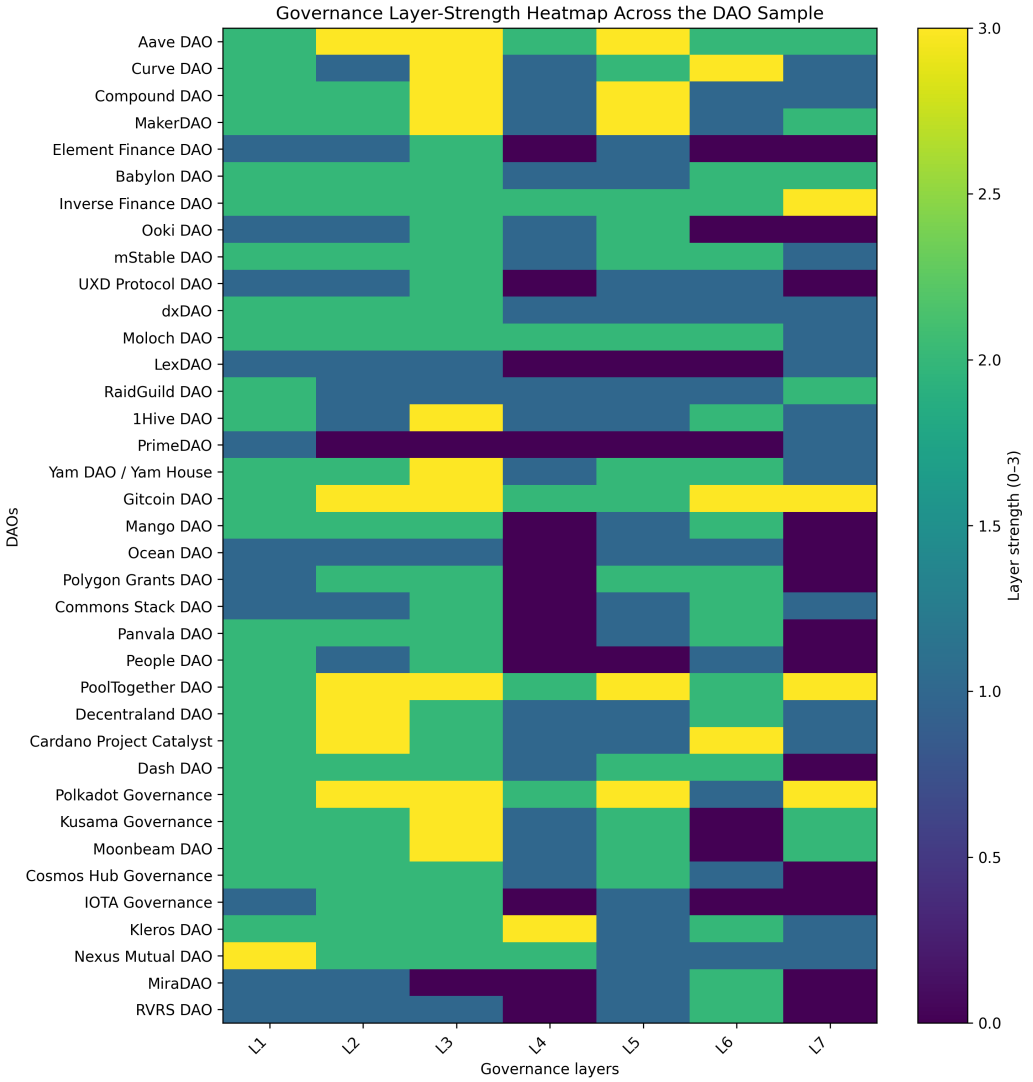


Figure 1. Heatmap of governance layer-strength scores across the thirty-seven DAOs. Rows represent DAOs and columns represent the seven governance layers. Darker intensity indicates stronger implementation on the 0–3 maturity scale.

The heatmap highlights two important empirical patterns. First, governance maturity is unevenly distributed across layers, confirming that broad governance coverage does not necessarily imply strong institutionalization across all governance functions. Second, the figure shows that DAOs with relatively strong collective choice and execution layers do not necessarily exhibit equally strong accountability or meta-governance structures. This pattern is consistent with prior empirical evidence that effective governance control often

diverges from formal governance design, particularly where participation is concentrated or safeguards are weakly specified [8,9].

These quantitative values should be interpreted in light of documentation visibility, as lower scores may in some cases reflect limited public traceability rather than the complete absence of governance practice.

4.7.6. Principal Empirical Findings

Taken together, the empirical application of the Governance Coverage Model supports four principal findings.

First, governance breadth does not imply governance maturity. Many DAOs implement several governance layers, but the strength of implementation varies substantially across layers and across DAO types. Second, technical governance layers, particularly collective choice and execution, tend to be more mature than socio-institutional layers such as accountability and legitimacy. Third, accountability and safeguard structures remain systematically underdeveloped, making them one of the clearest governance risk areas in the sample. Fourth, governance maturity is configuration-dependent: what matters is not only how many layers are present, but how they interact and whether critical institutional weaknesses remain exposed.

These findings provide direct empirical support for the Governance Coverage Model as an analytical framework. The model does not simply classify governance mechanisms; it identifies where DAO governance is institutionally robust, where it remains fragile, and why formally similar governance systems may differ substantially in maturity and resilience.

A further caution concerns the temporal interpretation of these findings. The present analysis is cross-sectional and does not include DAO age, founding date, crisis history, or governance lifecycle stage as coded variables. Accordingly, weak maturity in operational delegation and meta-governance (L7) should not be interpreted as permanent institutional immaturity. In some cases, a weak L7 score may reflect early-stage governance development, limited exposure to institutional stress, or the absence of prior governance crises that would otherwise motivate formal rule-evolution mechanisms. Conversely, older or more operationally complex DAOs may have stronger incentives to formalize meta-governance, but the present study does not test a statistical relationship between DAO longevity and L7 maturity. Future longitudinal work should examine whether meta-governance maturity emerges as a design choice, as a response to governance failures, or as a natural byproduct of organizational survival.

5. Implications and Perspectives of the Governance Coverage Model for Blockchain-Based IoT and AI Systems

Although the Governance Coverage Model was developed and empirically applied using active DAOs, its contribution is not limited to DAO-native organizational analysis. The model is also relevant to blockchain-based Internet of Things (IoT) and AI-enabled infrastructures, where governance maturity can influence security, reliability, resilience, data integrity, and operational trust. In these environments, governance is not simply a matter of voting over organizational preferences; it shapes who is authorized to participate, how infrastructure changes are approved, how incidents are escalated, how incentives affect behavior, and how system rules are enforced across heterogeneous devices, services, and data actors. Recent research on blockchain-enabled IoT emphasizes that decentralized infrastructures require technical mechanisms for traceability and tamper resistance, but also credible governance arrangements for coordinating participation, adaptation, and oversight across distributed actors [10–12].

From this perspective, the Governance Coverage Model provides a structured way to translate blockchain-governance analysis into IoT/security application contexts. The seven layers can be interpreted as governance functions that support trusted participation, secure rule change, accountable intervention, reliable enforcement, incentive integrity, and adaptive oversight. The following subsections extend the model in two directions: first, by interpreting governance maturity as a trust and resilience regime for blockchain-based IoT and AI systems and illustrating this through a DAO-governed IoT data marketplace; and second, by outlining how AI-enabled governance analytics may support monitoring, anomaly detection, and risk oversight in decentralized infrastructures.

5.1. Governance Maturity as a Trust and Resilience Regime

The Governance Coverage Model can be interpreted not only as a framework for analyzing DAO decision-making, but also as a trust and resilience regime for blockchain-based IoT and AI systems. In such environments, governance is closely tied to operational concerns including who is authorized to participate, how infrastructure changes are proposed and approved, how incidents are handled, how incentives shape system behavior, and how governance rules evolve in response to technical or organizational stress. Recent research on blockchain-enabled IoT emphasizes that secure and trustworthy decentralized operation depends not only on cryptographic guarantees and distributed ledgers, but also on effective coordination, validation, adaptability, and institutional control across heterogeneous actors and services [10–12].

From this perspective, governance maturity affects whether decentralized infrastructures remain reliable, auditable, and resilient over time. Participation and legitimacy influence trusted membership and authority boundaries; agenda control and collective choice shape the legitimacy and quality of infrastructure change; accountability and safeguards determine whether harmful actions can be contested or contained; execution and enforcement govern whether approved decisions are implemented reliably; incentive alignment and treasury governance affect the sustainability and integrity of participation; and operational delegation and meta-governance shape the system's capacity to adapt under changing technical and organizational conditions. In blockchain-based IoT and AI systems, governance maturity is therefore not merely an organizational property, but a system-level condition that contributes directly to trust establishment, security maintenance, and resilient decentralized operation.

Table 4 shows that the governance layers identified in the model are not only relevant to internal DAO coordination; they also map to core trust and resilience functions in decentralized infrastructures. This makes the Governance Coverage Model useful for interpreting the institutional robustness of blockchain-based IoT and AI systems beyond DAO-native governance settings.

In IoT- and security-oriented deployments, however, the seven layers may not carry equal operational consequences. While the aggregate maturity index used in the empirical analysis is intentionally unweighted for descriptive comparability, some layers may operate as high-criticality or gatekeeper layers in infrastructure settings. In particular, accountability and safeguard structures (L4) and execution and enforcement processes (L5) are especially important because failures in these layers can directly affect incident containment, compliance with approved rules, and the reliability of operational responses. A system may appear mature in participation, proposal formation, or voting, but still remain fragile if harmful actions cannot be contested or if approved decisions are not reliably enforced. Therefore, in blockchain-based IoT/AI systems, L4 and L5 may require additional scrutiny or domain-specific weighting when governance maturity is interpreted as a trust and resilience regime.

Table 4. Interpretation of governance maturity as a trust and resilience regime in blockchain-based IoT/AI systems.

Governance Layer	Trust/Resilience Function	Implication of Weak Maturity
Participation and legitimacy	Defines trusted participation and authority boundaries	Weak participant validation, exclusion disputes, or concentrated control
Agenda control and proposal formation	Structures legitimate change and operational updates	Opaque or capture-prone change requests
Collective choice mechanisms	Governs approval of shared operational decisions	Manipulated outcomes or weak decision legitimacy
Accountability and safeguard structures	Supports incident response, contestability, and intervention	Poor fault containment and weak recovery governance
Execution and enforcement	Ensures approved decisions are implemented reliably	Policy drift, weak compliance, or non-binding outcomes
Incentive alignment and treasury governance	Sustains honest participation and operational maintenance	Reward gaming, low-quality contribution, or resource misuse
Operational delegation and meta-governance	Enables adaptive and scalable oversight	Governance rigidity and weak long-term resilience

5.2. Illustrative Use Case: A DAO-Governed IoT Data Marketplace

To illustrate the broader applicability of the Governance Coverage Model, this subsection considers the case of a DAO-governed IoT data marketplace. The purpose of this use case is not to introduce a second empirical dataset, but to show how the model can be interpreted in a decentralized infrastructure where governance directly affects trust, risk oversight, data integrity, and operational reliability. IoT data marketplaces are a particularly suitable context because they involve multiple actors, continuous data exchange, economic incentives, access-control decisions, and recurring governance choices regarding participation, pricing, validation, dispute handling, and system evolution [10,11]. In such environments, blockchain can support transparency, traceability, and tamper-evident records, while DAO-based governance can provide a decentralized mechanism for establishing and revising marketplace rules [10,12].

5.2.1. General Description of the Use Case

A DAO-governed IoT data marketplace typically involves several categories of actors: (i) data providers, such as sensor owners or device operators who generate and publish data; (ii) gateway or infrastructure operators, who support connectivity, processing, or availability; (iii) data consumers, who access and use marketplace data; and (iv) governance participants, who collectively define and revise marketplace rules. Smart contracts may be used to register participants, record data-related transactions, enforce access or payment rules, and distribute rewards, while governance processes determine the institutional rules under which the marketplace operates.

The marketplace operates at the intersection of technical and institutional functions. On the technical side, devices generate and transmit data, access requests are processed, and transactions are logged. On the governance side, participants must determine who is eligible to contribute data, how data quality or legitimacy is verified, how pricing and access policies are changed, how malicious or low-quality behavior is handled, and how resources are allocated for maintenance, dispute resolution, or future development. As a result, governance is not external to the marketplace; rather, it becomes part of the operational structure through which the marketplace maintains trust and continuity.

Figure 2 presents a conceptual overview of this use case.

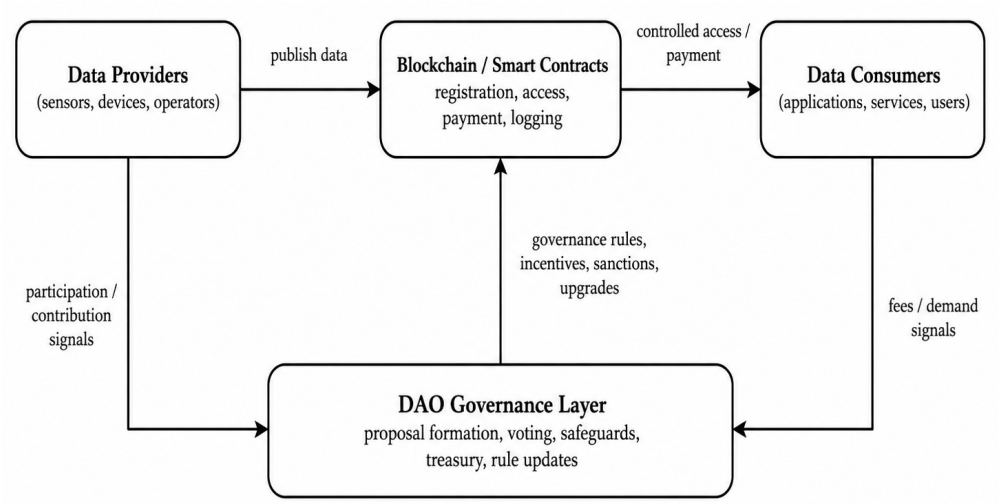


Figure 2. Conceptual view of a DAO-governed IoT data marketplace.

As shown in Figure 2, the DAO governance layer mediates the institutional structure of the marketplace by shaping who participates, how rules are revised, how incentives are distributed, and how irregular or harmful behavior is addressed. This makes the use case suitable for illustrating how the Governance Coverage Model can be applied beyond DAO-native organizational analysis.

The use case is therefore not only an example of decentralized marketplace coordination; it is also an IoT/security application context. Data integrity depends on whether data providers are admitted and monitored through credible participation rules. Reliability depends on whether access, pricing, validation, and update policies are revised through transparent and enforceable governance procedures. Security and risk oversight depend on whether malicious contribution, data misuse, or infrastructure abuse can be challenged, sanctioned, or contained. This makes the IoT data marketplace a useful application setting for demonstrating how governance maturity becomes operationally relevant to security, reliability, and data integrity in blockchain-based infrastructures.

5.2.2. Mapping the Use Case to the Governance Coverage Model

The Governance Coverage Model can be used to map the institutional functions required for a trustworthy and resilient IoT data marketplace. In this context, each governance layer corresponds to a concrete governance problem within marketplace operation, including participant admission, proposal formation, decision approval, dispute handling, enforcement, incentive design, and rule adaptation.

This layered interpretation is important because governance in an IoT data marketplace is not exhausted by voting over policies. A marketplace may have an explicit voting mechanism but still remain institutionally fragile if it lacks adequate safeguards against malicious data providers, effective enforcement of approved rules, or incentive structures that discourage low-quality contribution. Similarly, a marketplace may possess transparent payment rules yet remain vulnerable if participation rights are poorly specified or if governance cannot adapt when new technical risks emerge. Table 5 maps the seven governance layers to their corresponding roles and governance concerns in a DAO-governed IoT data marketplace.

As shown in Table 5, the governance of an IoT data marketplace spans the full lifecycle of decentralized coordination rather than a single decision mechanism. It includes admission control, proposal structuring, collective approval, dispute handling, economic oversight, operational enforcement, and institutional adaptation. The Governance Cover-

age Model therefore provides a systematic lens through which the governance design of such a marketplace can be examined as an integrated institutional architecture.

Table 5. Mapping of the Governance Coverage Model to a DAO-governed IoT data marketplace.

Governance Layer	Role in the IoT Data Marketplace	Illustrative Governance Concern
Participation and legitimacy	Defines who may join the marketplace as a data provider, validator, infrastructure operator, or governance participant	Untrusted or low-quality actors entering the marketplace; unclear participation rights
Agenda control and proposal formation	Determines who may propose changes to pricing, access rules, validation procedures, or marketplace parameters	Agenda capture, opaque rule-change processes, or proposal overload
Collective choice mechanisms	Governs how proposals are evaluated and approved through voting, delegation, or quorum rules	Weak decision legitimacy, concentrated influence, or low-quality collective choices
Accountability and safeguard structures	Provides mechanisms for disputes, sanctions, emergency intervention, or challenge procedures	Inability to respond to harmful data behavior, manipulation, or governance abuse
Execution and enforcement	Ensures approved decisions are translated into binding marketplace rules or contract-level actions	Policy drift, inconsistent implementation, or non-binding decisions
Incentive alignment and treasury governance	Shapes rewards, fees, treasury usage, and economic incentives for data contribution and infrastructure support	Reward gaming, poor-quality contribution, treasury misuse, or weak sustainability
Operational delegation and meta-governance	Supports committees, moderators, or specialized roles and enables future revision of governance rules	Governance rigidity, weak specialization, or inability to adapt to technical and regulatory change

5.2.3. Assessing Governance Maturity as Trust and Risk Oversight

In the context of a DAO-governed IoT data marketplace, governance maturity can be interpreted as the degree to which the governance architecture functions as an effective trust and risk oversight regime. Trust in this setting concerns confidence in who participates, how decisions are made, whether marketplace rules are implemented reliably, and whether data-related interactions are governed in a fair and auditable manner. Risk oversight concerns the system's capacity to detect, contain, and respond to governance failures, low-quality behavior, policy misuse, or institutional weaknesses that may undermine reliability, security, or data integrity [11,12].

The four-level layer-strength scale introduced earlier in the paper can be directly interpreted in this context. A score of 0 indicates that a governance function is not visibly supported or not publicly evidenced. A score of 1 indicates a weak or informal arrangement with limited binding effect. A score of 2 indicates that the function is defined and used, but remains only partially robust or incompletely enforced. A score of 3 indicates that the governance function is explicit, auditable, regularly exercised, and designed with visible safeguards against relevant threats. In a DAO-governed IoT data marketplace, such scores do not merely indicate governance sophistication; they indicate the extent to which the marketplace can sustain trusted participation and credible risk oversight.

From this perspective, higher governance maturity implies that trust and oversight are institutionally embedded rather than dependent on informal assumptions. A mature governance architecture helps ensure that data contribution is linked to legitimate participation, policy changes are introduced and approved transparently, harmful behavior can be contested, approved rules are enforceable, and incentives do not undermine marketplace integrity. Conversely, weak governance maturity increases the likelihood that technical trust mechanisms alone will be insufficient to prevent governance failures, economic ma-

nipulation, or long-term institutional fragility. Table 6 summarizes how each governance layer can be interpreted as a trust and risk oversight function in a DAO-governed IoT data marketplace.

Table 6. Illustrative interpretation of governance maturity as trust and risk oversight in a DAO-governed IoT data marketplace.

Governance Layer	Trust/Risk Oversight Function	Illustrative Indicator of Higher Maturity
Participation and legitimacy	Establishes confidence in who may contribute, validate, or govern	Clear admission rules, traceable membership criteria, and credible participant validation
Agenda control and proposal formation	Reduces arbitrary or captured rule changes	Transparent proposal pipeline, clear proposal eligibility, and auditable proposal stages
Collective choice mechanisms	Supports legitimate and reviewable collective decision-making	Defined voting rules, visible quorum thresholds, and repeated evidence of governance participation
Accountability and safeguard structures	Enables challenge, intervention, and containment of harmful behavior	Dispute procedures, emergency safeguards, or documented sanction/intervention mechanisms
Execution and enforcement	Ensures that approved rules affect actual marketplace operation	Reliable smart-contract execution, timelocks, or explicit link between vote outcomes and implementation
Incentive alignment and treasury governance	Protects economic integrity and contribution quality	Transparent reward distribution, visible treasury controls, and anti-gaming incentive design
Operational delegation and meta-governance	Supports scalable oversight and adaptation under change	Documented committees or delegated roles and clear mechanisms for modifying governance rules

Accordingly, the Governance Coverage Model offers a useful analytical framework for examining whether a DAO-governed IoT data marketplace is institutionally mature enough to support decentralized trust. It enables evaluation not only of whether governance mechanisms exist, but also of whether they are sufficiently robust to function as a credible trust and risk oversight regime in a data-intensive blockchain-based infrastructure.

5.3. AI-Enabled Governance Analytics and Risk Oversight

A further implication of the Governance Coverage Model concerns the role of artificial intelligence and data-driven analytics in supporting governance oversight within blockchain-based IoT and AI systems. As decentralized infrastructures scale, governance increasingly generates large and heterogeneous streams of events, including proposal submissions, voting behavior, delegation changes, treasury movements, smart-contract execution traces, and infrastructure-related operational signals. Recent research suggests that AI can enhance blockchain-based systems through monitoring, anomaly detection, smart-contract analysis, and decision support [14,61]. At the same time, computational analyses of DAO ecosystems indicate that governance activity itself can be studied through data-driven approaches, including trend analysis, topic extraction, and large-scale behavioral interpretation [15]. These developments make it reasonable to interpret AI not as a substitute for legitimate collective governance, but as an assistive governance analytics layer that can strengthen oversight and adaptive response.

Within the proposed model, AI-enabled governance analytics can support three interrelated functions. First, it can enhance *governance monitoring* by continuously analyzing governance-event streams for patterns such as proposal congestion, declining participation,

abnormal delegate concentration, or unusual treasury behavior. Second, it can support *risk detection* by identifying signals associated with governance capture, collusive voting, abrupt concentration of influence, suspicious contract-level behavior, or operational deviations relevant to DAO-governed infrastructures [61,62]. Third, it can support *decision assistance* by summarizing proposals, clustering governance issues, highlighting emerging governance bottlenecks, and generating interpretable alerts for delegates, committees, or broader communities. In this sense, AI becomes a complementary mechanism for observing the operational health of the governance layers rather than a replacement for those layers themselves.

This perspective is especially relevant in blockchain-based IoT environments, where governance decisions may affect not only treasury allocation or voting outcomes, but also trusted participation, infrastructure reliability, incident response, and the integrity of system updates. In such settings, AI analytics can help connect technical and governance signals. For example, anomalies in smart-contract execution or access-control behavior may indicate weaknesses in execution and enforcement, while unusual voting patterns or concentrated proposal success rates may indicate weaknesses in collective choice, participation legitimacy, or accountability structures. Research on blockchain and AI-based trust management in IoT similarly suggests that intelligent analytics can play an important role in supporting trust evaluation, adaptive security, and risk-aware system coordination [12].

The conceptual role of AI-enabled governance analytics in the present study is therefore not prescriptive automation, but structured oversight. The Governance Coverage Model defines the institutional functions that should exist in a resilient decentralized governance architecture, whereas AI-enabled analytics can help observe whether those functions are operating in a healthy, transparent, and risk-aware manner.

Figure 3 presents a conceptual view of this relationship. It shows that AI-enabled governance analytics operates as an intermediate interpretive layer between raw governance and infrastructure signals on the one hand and institutional oversight actions on the other. The purpose of this layer is to transform heterogeneous governance-related events into interpretable indicators of concentration, anomaly, fragility, or emerging risk. These indicators may then inform governance responses such as proposal review, safeguard activation, treasury scrutiny, or rule revision. This interpretation is consistent with recent work on AI-supported blockchain governance, anomaly detection, and machine-learning-based smart-contract analysis, all of which emphasize the value of intelligent monitoring and explainable risk identification in decentralized environments [62–64].

A critical issue is that the AI-enabled analytics layer must itself be governed. If the analytics system is controlled by a narrow set of actors, configured through opaque thresholds, or updated without collective oversight, it may become a new vector for agenda capture, algorithmic bias, or centralized control. Therefore, AI-enabled governance analytics should be treated as a governed decision-support layer rather than as an autonomous authority. Its data sources, model-selection procedures, risk thresholds, update cycles, access rights, and alerting rules should be subject to explicit governance procedures. In terms of the Governance Coverage Model, this means that the AI layer should be governed through agenda control (L2), collective approval or delegated authorization (L3/L7), accountability and safeguards (L4), and auditable enforcement rules (L5).

This interpretation also addresses the incentive problem of AI-enabled oversight. The actors who maintain the analytics layer may have incentives to shape what is monitored, how risks are scored, or which alerts receive attention. To reduce this risk, the governance of the AI layer should include transparent documentation, audit trails, contestability of alerts, separation between analytics providers and final decision-makers, and periodic review of model performance. In this way, AI analytics can improve governance observability

without becoming a substitute for legitimate collective choice or a new mechanism of centralized control.

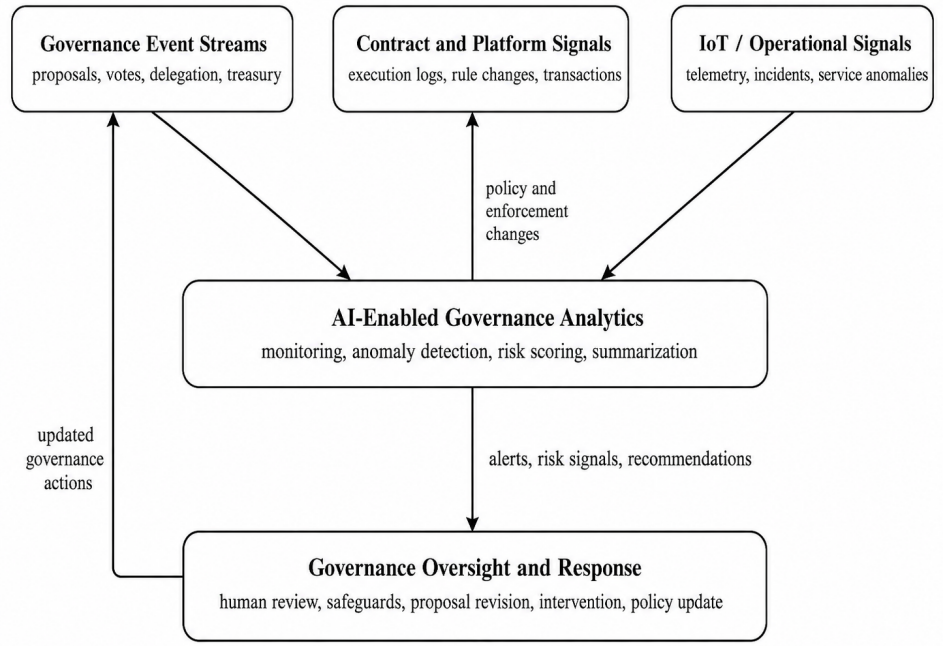


Figure 3. Conceptual framework of AI-enabled governance analytics and risk oversight in DAO-governed blockchain-based infrastructures.

The relationship between the analytics layer and the Governance Coverage Model can also be expressed more directly. Participation and legitimacy may be monitored through participation dispersion, validator concentration, or contributor turnover. Agenda control and proposal formation may be monitored through proposal volume, rejection rates, or agenda concentration. Collective choice mechanisms may be monitored through turnout dynamics, delegate dominance, or unusual voting alignment. Accountability and safeguard structures may be monitored through the frequency and handling of disputes, interventions, or unresolved anomalies. Execution and enforcement may be observed through the alignment between approved decisions and on-chain implementation. Incentive alignment and treasury governance may be monitored through reward concentration, irregular disbursement patterns, or economically suspicious behavior. Operational delegation and meta-governance may be monitored through committee activity, governance latency, or delayed rule adaptation.

Table 7 summarizes this interpretive mapping. It reinforces the idea that AI-enabled analytics does not replace institutional governance; rather, it improves the observability of governance maturity. In this way, the Governance Coverage Model remains the normative and analytical foundation of governance evaluation, while AI-enabled analytics functions as a complementary mechanism for monitoring whether governance layers are operating with sufficient robustness, transparency, and responsiveness. This perspective is particularly useful for blockchain-based IoT and AI systems, where the scale, heterogeneity, and event intensity of decentralized infrastructures may otherwise make governance weaknesses difficult to detect before they affect trust, security, resilience, or data integrity. However, AI-enabled analytics should remain a transparent and contestable support mechanism governed by the same institutional principles that the Governance Coverage Model identifies, rather than an independent authority over decentralized governance.

Table 7. Illustrative role of AI-enabled governance analytics across the governance layers.

Governance Layer	Illustrative Analytics Focus	Example Risk Signal
Participation and legitimacy	Participation dispersion, actor concentration, contributor turnover	Persistent dominance by a narrow set of actors or weak membership diversity
Agenda control and proposal formation	Proposal volume, proposal source concentration, proposal bottlenecks	Agenda capture, excessive proposal congestion, or low proposal accessibility
Collective choice mechanisms	Voting turnout, delegate influence, unusual voting alignment	Collusive patterns, unusually concentrated voting outcomes, or legitimacy erosion
Accountability and safeguard structures	Dispute frequency, intervention triggers, unresolved incidents	Missing safeguards, delayed intervention, or repeated unresolved governance failures
Execution and enforcement	Alignment between approved decisions and executed actions	Policy drift, delayed implementation, or weak enforcement consistency
Incentive alignment and treasury governance	Reward concentration, treasury outliers, disbursement anomalies	Incentive gaming, suspicious treasury movement, or funding misuse
Operational delegation and meta-governance	Committee activity, governance delay, rule-update frequency	Governance rigidity, poor adaptive response, or oversight overload

6. Discussion

This study addressed a central limitation in DAO governance research: the tendency to evaluate decentralized governance through isolated mechanisms, particularly voting, rather than through the broader institutional architecture within which those mechanisms operate. The empirical application of the Governance Coverage Model shows that governance breadth and governance maturity are analytically distinct. Across the thirty-seven DAOs examined, many systems visibly implement multiple governance mechanisms, yet the strength, enforceability, and resilience of these mechanisms vary substantially across layers. This supports the core premise of the paper: DAO governance is better understood as a layered institutional system than as a set of discrete technical tools.

The results indicate that governance effectiveness depends less on the presence of a single decision rule and more on the interaction among governance layers. Prior research has questioned the adequacy of mechanism-specific evaluation, particularly where voting rights are formally distributed but substantively concentrated [4,6,9]. The present findings extend this argument by showing that voting and execution layers are generally more mature than legitimacy, safeguards, and meta-governance. This suggests that many DAOs develop decision capacity before developing commensurate institutional constraints. A governance system that can decide and execute, but cannot adequately constrain, contest, or adapt those decisions, remains institutionally fragile.

The findings also refine the interpretation of decentralization in DAO governance. Decentralization should not be treated as a property that automatically follows from open participation, tokenized voting, or on-chain execution. A DAO may be decentralized in execution but concentrated in participation; procedurally open but weak in accountability; or operationally active while lacking mature meta-governance. This interpretation is consistent with empirical work showing that formal governance openness may coexist with concentrated voting power and limited effective control by the broader membership [8,9]. The Governance Coverage Model therefore contributes a more precise vocabulary for analyzing decentralization as a multidimensional institutional condition.

One of the clearest empirical observations is the weakness of accountability and safeguard structures. Accountability and safeguards (L4) emerged as the least mature layer, while operational delegation and meta-governance (L7) also remained compara-

tively underdeveloped. This finding suggests that governance risks are not explained only by participation rates, voting design, or incentive structure. They also arise from weak constraint mechanisms. Where veto processes, challenge procedures, emergency controls, or structured dispute mechanisms are absent or weak, DAOs remain exposed to capture, malicious proposals, and strategic manipulation even when voting procedures are well formalized [7,8,21].

The category-level comparison indicates that governance maturity is partly shaped by DAO function. Protocol-oriented and infrastructure-oriented DAOs exhibit higher aggregate maturity than organizational and guild-oriented or mission- and funding-oriented DAOs. This pattern is plausible because protocol and infrastructure systems often depend on auditable rule changes, on-chain execution, and repeatable proposal procedures. However, these differences should not be read as a simple ranking of superior and inferior DAO types. They should be interpreted as differences in publicly verifiable governance maturity, shaped by both institutional design and documentation visibility.

This qualification is important because the study's evidence strategy introduces a potential documentation bias. The scoring protocol relies on publicly available and traceable governance artifacts, which improves reproducibility but may understate the maturity of DAOs whose governance practices are sophisticated yet informal, socially embedded, or weakly documented. Protocol and infrastructure DAOs often expose formal governance documentation, on-chain execution records, and public proposal archives, whereas mission-oriented, funding-oriented, organizational, or guild-based DAOs may rely more heavily on norms, working groups, and off-chain deliberation. Thus, part of the observed maturity gap may reflect visibility asymmetry rather than substantive institutional weakness. The results should therefore be interpreted as evidence of publicly verifiable governance maturity, not as a complete ranking of all formal and informal governance capacity.

The cross-sectional design also requires caution. The study captures governance maturity at one point in time and does not model DAO age, founding date, crisis history, or lifecycle stage. This is particularly relevant to L7, operational delegation and meta-governance. A weak L7 score may indicate immature rule-evolution capacity, but it may also reflect a young DAO that has not yet faced the institutional stress or governance crisis needed to formalize meta-governance. Future longitudinal work should examine whether meta-governance emerges as an intentional design choice, a response to governance failure, or a byproduct of organizational survival.

The aggregate maturity index should likewise be interpreted as a descriptive baseline. The unweighted sum preserves transparency and comparability across heterogeneous DAOs, but it does not imply that all layers are equally consequential in every context. In security-sensitive or infrastructure-oriented deployments, accountability and safeguards (L4) and execution and enforcement (L5) may function as gatekeeper layers. A system may appear mature in participation, agenda formation, or voting, but remain fragile if harmful actions cannot be contested or approved decisions are not reliably enforced.

This gatekeeper interpretation is especially important in blockchain-based IoT and AI systems. In such environments, governance failures may affect not only treasury allocation or decision legitimacy, but also service continuity, trusted participation, incident response, security, and data integrity. The IoT data marketplace use case illustrates how weak participation controls, captured proposal formation, absent safeguards, or unreliable enforcement can undermine the operational trust architecture of a decentralized infrastructure. In this sense, governance maturity becomes a system-level condition for trust and resilience, not merely an organizational property of DAOs [10–12].

The AI-enabled governance analytics extension further broadens the model's relevance. The paper does not treat AI as a substitute for legitimate collective governance;

rather, it positions analytics as an assistive oversight layer that may improve the observability of governance maturity through monitoring, anomaly detection, smart-contract analysis, and decision support [14,15,61,62]. However, the analytics layer must itself be governed. If controlled by a narrow set of actors or updated through opaque procedures, it may become a new vector for capture, bias, or centralized control. Therefore, the data sources, model-selection procedures, thresholds, alerting rules, access rights, and update cycles of AI-enabled analytics should be transparent, contestable, and subject to institutional safeguards.

The study has practical implications for DAO designers and developers of blockchain-based IoT/AI infrastructures. DAO designers should avoid equating active voting with mature governance and should give greater attention to accountability, intervention mechanisms, participation quality, and meta-governance. For blockchain-based IoT and AI systems, the implications are more operational: participation rules affect who may contribute data or operate infrastructure; proposal and voting procedures affect system changes; safeguards affect response to anomalies; enforcement affects whether approved policies become actual system behavior; and incentives affect data quality and long-term sustainability.

Despite its contributions, the study has limitations. It relies on publicly available governance artifacts and may therefore be affected by documentation bias. It is cross-sectional and does not explain temporal evolution or causal effects. The four-level strength scale is ordinal and does not capture all nuances of governance practice. Finally, the aggregate maturity index is intentionally unweighted and should be interpreted as a descriptive baseline rather than a risk-weighted measure. Future research should extend the model through longitudinal analysis, outcome-oriented validation, weighted or gatekeeper-based variants for security-critical deployments, and governance-aware analytics using event streams, treasury traces, operational telemetry, or proposal histories.

Overall, the discussion reinforces the central contribution of the paper. DAO governance should not be understood as synonymous with token voting, treasury allocation, or proposal execution. It is better understood as a layered institutional architecture whose robustness depends on the coordinated maturity of participation, agenda formation, collective choice, safeguards, execution, incentives, and meta-governance. The Governance Coverage Model provides a structured way to make this architecture visible, comparable, and empirically analyzable, while also offering a broader framework for interpreting trust, resilience, risk oversight, and governance maturity in blockchain-based IoT and AI systems.

7. Conclusions

This study introduced the Governance Coverage Model as a layered framework for evaluating DAO governance beyond isolated mechanisms such as voting. The model conceptualizes DAO governance as seven interdependent institutional functions: participation and legitimacy, agenda control, collective choice, accountability and safeguards, execution and enforcement, incentive alignment and treasury governance, and operational delegation and meta-governance. By combining this layered structure with a four-level strength scale, the model enables a more systematic assessment of governance maturity than binary presence-or-absence evaluation.

The paper also clarified the model's specification and boundaries. The seven functions were selected because they recur across DAO governance literature, jointly cover the lifecycle of decentralized decision-making, are empirically observable through governance artifacts, and remain analytically separable. Related concepts such as transparency, decentralization, trust, inclusiveness, and security are treated as cross-cutting properties or outcomes rather than standalone layers. This keeps the model focused on governance

architecture while allowing it to support broader interpretation in decentralized infrastructure contexts.

The empirical application to thirty-seven active DAOs showed that governance breadth does not necessarily imply governance maturity. Collective choice and execution mechanisms are generally more developed than accountability, safeguards, and meta-governance, suggesting that many DAOs develop decision capacity faster than institutional constraint and adaptive governance capacity. Category-level results further indicate that protocol-oriented and infrastructure-oriented DAOs exhibit higher publicly verifiable maturity than organizational and guild-oriented or mission- and funding-oriented DAOs.

These findings should be interpreted with caution. Because the scoring relies on publicly available governance artifacts, lower scores may partly reflect limited documentation visibility rather than the absence of governance practice. This may especially affect DAOs that rely on informal, socially embedded, or off-chain governance processes. In addition, the analysis is cross-sectional and does not test whether DAO age, crisis history, or lifecycle stage influences maturity, particularly in relation to meta-governance. The aggregate maturity index is also intentionally unweighted and should be understood as a descriptive baseline rather than a complete risk-weighted measure.

The study contributes in three ways. First, it provides a formal and empirically operational framework for comparing DAO governance architectures. Second, it offers evidence that governance robustness is best understood as a configuration of interacting institutional layers rather than as the presence of individual tools. Third, it extends the relevance of the model to blockchain-based IoT and AI systems by interpreting governance maturity as a trust and resilience regime affecting security, reliability, data integrity, incident response, and adaptive oversight.

In this broader context, accountability and safeguards (L4) and execution and enforcement (L5) may operate as gatekeeper layers in security-sensitive IoT/AI deployments. Similarly, AI-enabled governance analytics may support monitoring, anomaly detection, and risk oversight, but the analytics layer must itself be governed through transparent procedures, contestable outputs, safeguards, and meta-governance. Overall, the Governance Coverage Model offers a structured foundation for future empirical and comparative research on DAO governance and a practical instrument for evaluating the institutional resilience of trusted, secure, and accountable decentralized infrastructures.

Author Contributions: Conceptualization, A.S.A.-H.; methodology, A.S.A.-H.; validation, A.S.A.-H. and R.A.; formal analysis, A.S.A.-H.; investigation, A.S.A.-H.; resources, R.A.; data curation, R.A. and A.S.A.-H.; writing—original draft preparation, A.S.A.-H.; writing—review and editing, A.S.A.-H.; visualization, A.S.A.-H.; supervision, A.S.A.-H.; project administration, A.S.A.-H.; funding acquisition, A.S.A.-H. and R.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Raw data are available at https://3339.notion.site/Governance-28513f5830d144ea9202bf7c64558c9d (accessed on 2 June 2026). The DAO-by-layer governance matrix, layer-summary statistics, and figure source data generated during this study are available from the corresponding author upon reasonable request.

Acknowledgments: During the preparation of this manuscript, the authors used ChatGPT (GPT-5.2) to assist with spelling and grammar correction, as well as to review the consistency and coherence of the manuscript. The authors carefully reviewed and edited all generated output and take full responsibility for the content of this publication.

Conflicts of Interest: Rand Alkharashi was the founder of Quintes Protocol, a real-world asset tokenization research and engineering effort. There is no commercial relationship between Quintes Protocol and the manuscript. Author Rand Alkharashi is employed by Innovative Technologies. The remaining author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

DAO	Decentralized Autonomous Organization
IoT	Internet of Things
AI	Artificial Intelligence

Appendix A. Governance Layer Scoring Rubric

This appendix summarizes the operational rubric used to assign layer-strength scores in the Governance Coverage Model. The rubric supports methodological transparency by providing concise interpretation anchors for the seven governance layers and the four ordinal scores used in the empirical analysis. Scores were assigned only on the basis of publicly verifiable governance artifacts; therefore, a score of 0 indicates the absence of explicit public evidence rather than definitive proof that the function is absent in informal practice.

Table A1. Governance layer scoring rubric used in the empirical analysis.

Governance Layer	0—Not Available	1—Weak	2—Moderate	3—Strong
Participation & Legitimacy	No explicit public evidence of participation rules	Informal or symbolic inclusion	Repeated participation with limits	Auditable inclusion with anti-capture design
Agenda Control & Proposal Formation	No explicit public evidence of a proposal process	Discretionary or unclear rules	Formal proposal pipeline	Transparent pipeline with agenda safeguards
Collective Choice Mechanisms	No explicit public evidence of a voting mechanism	Basic voting with limited safeguards	Documented voting in practice	Robust aggregation with anti-whale/collusion design
Accountability & Safeguards	No explicit public evidence of safeguards	Informal social checks	Explicit but partial safeguards	Auditable, threat-aware safeguards
Execution & Enforcement	No binding execution evidence	Weak or informal execution	Hybrid or partially binding execution	Fully binding and auditable execution
Incentive Alignment & Treasury Governance	No explicit incentive or treasury structure	Implicit incentives only	Formal incentives with residual risks	Anti-capture and auditable economic design
Operational Delegation & Meta-Governance	No explicit delegation or rule-evolution process	Informal delegation	Documented delegation structures	Auditable delegation and adaptive rule evolution

The rubric was applied together with the evidence rules described in the main text: explicitness, auditability, threat-aware justification, and non-inference. Scores above 1 required traceable evidence of repeated use or enforceability, while score 3 was reserved for mechanisms that were explicit, auditable, and visibly designed to mitigate governance threats relevant to the layer. This conservative approach improves reproducibility while acknowledging that informal or weakly documented governance practices may be underrepresented.

References

1. Santana, C.; Albareda, L. Blockchain and the emergence of decentralized autonomous organizations (DAOs): An integrative model and research agenda. *Technol. Forecast. Soc. Change* **2022**, *182*, 121806. [CrossRef]
2. Hassan, S.; De Filippi, P. Decentralized autonomous organization. *Internet Policy Rev.* **2021**, *10*, 1–10. [CrossRef]

3. van Vulpen, P.; Siu, J.; Jansen, S. Governance of decentralized autonomous organizations that produce open source software. *Blockchain Res. Appl.* **2024**, *5*, 100166. [CrossRef]
4. Han, J.; Lee, J.; Li, T. A review of DAO governance: Recent literature and emerging trends. *J. Corp. Financ.* **2025**, *91*, 102734. [CrossRef]
5. Ding, Q.; Liebau, D.; Wang, Z.; Xu, W. A survey on decentralized autonomous organizations (DAOs) and their governance. *World Sci. Annu. Rev. Fintech* **2023**, *1*, 2350001. [CrossRef]
6. Liu, Y.; Lu, Q.; Zhu, L.; Paik, H.-Y.; Staples, M. A systematic literature review on blockchain governance. *J. Syst. Softw.* **2023**, *197*, 111576. [CrossRef]
7. Polcumpally, A.T.; Pandey, K.K.; Kumar, A.; Samadhiya, A. Blockchain governance and trust: A multi-sector thematic systematic review and exploration of future research directions. *Heliyon* **2024**, *10*, e32975. [CrossRef]
8. Fritsch, R.; Müller, M.; Wattenhofer, R. Analyzing voting power in decentralized governance: Who controls DAOs? *Blockchain Res. Appl.* **2024**, *5*, 100208. [CrossRef]
9. Barbereau, T.; Smethurst, R.; Papageorgiou, O.; Sedlmeir, J.; Fridgen, G. Decentralised Finance's timocratic governance: The distribution and exercise of tokenised voting rights. *Technol. Soc.* **2023**, *73*, 102251. [CrossRef]
10. Khan, I.; Majib, Y.; Ullah, R.; Rana, O. Blockchain applications for Internet of Things—A survey. *Internet Things* **2024**, *27*, 101254. [CrossRef]
11. Arshad, Q.-u.-A.; Khan, W.Z.; Azam, F.; Khan, M.K.; Yu, H.; Zikria, Y.B. Blockchain-based decentralized trust management in IoT: Systems, requirements and challenges. *Complex Intell. Syst.* **2023**, *9*, 6155–6176. [CrossRef]
12. D'Aniello, G.; Fotia, L. Blockchain and AI-based methods for trust management in IoT: A comprehensive survey. *Internet Things* **2025**, *34*, 101755. [CrossRef]
13. Cabello, C.; Mikalef, P. Exploring decentralized autonomous organization (DAO) governance: An integrative literature review. In Proceedings of the 16th Mediterranean Conference on Information Systems (MCIS 2024), Porto, Portugal, 3–5 October 2024; Paper 27.
14. Ressi, D.; Romanello, R.; Piazza, C.; Rossi, S. AI-enhanced blockchain technology: A review of advancements and opportunities. *J. Netw. Comput. Appl.* **2024**, *225*, 103858. [CrossRef]
15. Park, H.; Ureta, I.; Kim, B. Trend analysis of decentralized autonomous organization using big data analytics. *Information* **2023**, *14*, 326. [CrossRef]
16. Zhu, G.; He, D.; An, H.; Luo, M.; Peng, C. The governance technology for blockchain systems: A survey. *Front. Comput. Sci.* **2024**, *18*, 182813. [CrossRef]
17. Bellavitis, C.; Momtaz, P.P. Voting Governance and Value Creation in Decentralized Autonomous Organizations (DAOs). *J. Bus. Ventur. Insights* **2025**, *23*, e00537. [CrossRef]
18. Monteiro, T.D.; Sanchez, O.P.; Moraes, G.H.S.M. Exploring Off-Chain Voting and Blockchain in Decentralized Autonomous Organizations. *RAUSP Manag. J.* **2024**, *59*, 335–349. [CrossRef]
19. Dursun, T.; Üstündağ, B.B. A novel framework for policy based on-chain governance of blockchain networks. *Inf. Process. Manag.* **2021**, *58*, 102556. [CrossRef]
20. Dimitri, N. Quadratic voting in blockchain governance. *Information* **2022**, *13*, 305. [CrossRef]
21. Tamai, S.; Kasahara, S. DAO voting mechanism resistant to whale and collusion problems. *Front. Blockchain* **2024**, *7*, 1405516. [CrossRef]
22. Allen, D.W.E.; Berg, C.; Lane, A.M.; MacDonald, T.; Potts, J. The exchange theory of Web3 governance. *Kyklos* **2023**, *76*, 659–675. [CrossRef]
23. Pasquini, R.A. Quadratic Funding and Matching Funds Requirements. *SSRN Electron. J.* **2020**, 1–49. [CrossRef]
24. Aave DAO. Governance Documentation. Available online: https://governance.aave.com (accessed on 15 January 2026).
25. Compound Labs. Compound Governance. Available online: https://compound.finance/governance (accessed on 15 January 2026).
26. MakerDAO. Maker Governance Portal. Available online: https://vote.makerdao.com/ (accessed on 2 June 2026).
27. Curve Finance. Curve DAO Governance. Available online: https://gov.curve.finance/ (accessed on 2 June 2026).
28. Element Finance. Governance Documentation. Available online: https://gov.element.fi/en-US/proposals (accessed on 2 June 2026).
29. Babylon Foundation. Babylon Genesis Governance Guide. Available online: https://forum.babylon.foundation/t/governance-docs/19 (accessed on 2 June 2026).
30. Inverse Finance. Governance Documentation. Available online: https://docs.inverse.finance/inverse-finance/inverse-finance/governance (accessed on 2 June 2026).
31. Ooki Protocol. Official Smart-Contract Repository. Available online: https://github.com/OokiTrade/contractsV2 (accessed on 2 June 2026).
32. mStable. Governance Documentation. Available online: https://docs.mstable.org (accessed on 2 June 2026).

33. UXD Protocol. Governance Token UXP. Available online: https://docs.uxd.fi/uxdprotocol/overview/governance-token-uxp (accessed on 2 June 2026).
34. dxDAO. Governance Framework. Available online: https://dxdao.eth.link/ (accessed on 2 June 2026).
35. Moloch DAO. Framework Documentation. Available online: https://molochdao.com (accessed on 2 June 2026).
36. LexDAO. Membership and Governance. Available online: https://lexdao.org/membership/ (accessed on 2 June 2026).
37. RaidGuild. DAO Governance. Available online: https://raidguild.org (accessed on 2 June 2026).
38. 1Hive. Governance Portal. Available online: https://1hive.org (accessed on 2 June 2026).
39. PrimeDAO. Governance Documentation. Available online: https://primedao.eth.link (accessed on 2 June 2026).
40. Yam Finance. Governance Documentation. Available online: https://yam.finance (accessed on 2 June 2026).
41. Gitcoin DAO. Governance Portal. Available online: https://gov.gitcoin.co/ (accessed on 2 June 2026).
42. Blockworks Foundation. Mango Documentation Repository. Available online: https://github.com/blockworks-foundation/mango-docs (accessed on 2 June 2026).
43. Ocean Protocol. OceanDAO Round 9. Available online: https://oceanprotocol.com/press/2021-08-25-oceandao-round-9-300kusd-data-driven-projects (accessed on 2 June 2026).
44. Polygon. Polygon Governance Fundamentals. Available online: https://docs.polygon.technology/pos/governance/governance-fundamentals (accessed on 2 June 2026).
45. Commons Stack. Governance Framework. Available online: https://commonsstack.org (accessed on 2 June 2026).
46. Panvala. Governance Repository. Available online: https://github.com/Panvala/panvala (accessed on 2 June 2026).
47. PeopleDAO. Governance and Projects. Available online: https://people-dao.com/ (accessed on 2 June 2026).
48. PoolTogether. Governance Documentation. Available online: https://docs.pooltogether.com/pooltogether/governance (accessed on 2 June 2026).
49. Decentraland. DAO Governance Portal. Available online: https://decentraland.org/governance/ (accessed on 2 June 2026).
50. Cardano Foundation. Project Catalyst Governance. Available online: https://docs.projectcatalyst.io/ (accessed on 2 June 2026).
51. Dash Core Group. Dash DAO Governance. Available online: https://docs.dash.org/en/stable/ (accessed on 2 June 2026).
52. Web3 Foundation. Polkadot Governance. Available online: https://wiki.polkadot.com/ (accessed on 2 June 2026).
53. Web3 Foundation. Kusama Governance. Available online: https://wiki.polkadot.com/kusama/kusama-getting-started/ (accessed on 2 June 2026).
54. Moonbeam Network. Governance Documentation. Available online: https://docs.moonbeam.network (accessed on 2 June 2026).
55. Kleros. Governance and Arbitration Protocol. Available online: https://kleros.io (accessed on 2 June 2026).
56. MiraDAO. Governance Documentation. Available online: https://miradao.org (accessed on 2 June 2026).
57. RVRS DAO. RVRS DAO Climate Impact Initiative. Available online: https://reverseclimatechange.com/trust/ (accessed on 2 June 2026).
58. Cosmos Hub. Governance Documentation. Available online: https://hub.cosmos.network (accessed on 2 June 2026).
59. IOTA Foundation. IOTA Token Governance. Available online: https://docs.iota.org/about-iota/tokenomics/iota-token (accessed on 2 June 2026).
60. Nexus Mutual. Governance Documentation. Available online: https://docs.nexusmutual.io (accessed on 2 June 2026).
61. Shevchuk, R.; Martsenyuk, V.; Adamyk, B.; Benson, V.; Melnyk, A. Anomaly Detection in Blockchain: A Systematic Review of Trends, Challenges, and Future Directions. *Appl. Sci.* **2025**, *15*, 8330. [CrossRef]
62. Morar, C.D.; Popescu, D.E.; Novac, O.C.; Ghiurău, D. Rethinking Blockchain Governance with AI: The VOPPA Framework. *Computers* **2025**, *14*, 425. [CrossRef]
63. Ressi, D.; Spanò, A.; Benetollo, L.; Bugliesi, M.; Piazza, C.; Rossi, S. Vulnerability Detection in Solidity Smart Contracts via Machine Learning: A Qualitative Analysis. *Blockchain Res. Appl.* **2025**, 100390. [CrossRef]
64. Ibba, G.; Neykova, R.; Ortu, M.; Tonelli, R.; Counsell, S.; Destefanis, G. A machine learning approach to vulnerability detection combining software metrics and topic modelling: Evidence from smart contracts. *Mach. Learn. Appl.* **2025**, *22*, 100759. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.