

Autonomous competence identification protocol

Tim Pechersky

October 24, 2024

Abstract

This paper introduces a novel protocol for establishing ranking systems in decentralized autonomous organizations (DAOs) and consensus-building protocols. Leveraging cryptographic and social science insights, the protocol enables autonomous decision-making in trustless environments based on agent interactions. A real-world case study demonstrates the protocol’s potential to achieve high participation and retention rates, even without explicit incentives. The proposed protocol addresses key challenges in autonomous governance, such as low participation, centralization, and lack of commitment mechanisms, by fostering a more engaging, equitable, and secure decision-making process. It also has potential applications in various domains beyond DAOs, including decentralized social networks, academic research, and online education.

1 Introduction

The quest for consensus, a cornerstone of collective decision-making, has deep historical roots. From the ancient Chinese concept of *zhongyong* 中庸, advocating for moderation and balance in governance, to the Roman Republic’s emphasis on *senatus consulta* (senate decrees) reached through deliberation and compromise, societies have long grappled with the challenge of aligning diverse perspectives towards a common goal. The study of these historical precedents continues to inform modern approaches to consensus [1] [2].

The pursuit of consensus, has gained renewed significance in the digital age. Originating from the Bitcoin whitepaper [3], blockchain technology fundamentally seeks consensus and establishes trustless systems through cryptographic signatures. While significant progress has been made in developing efficient Byzantine Fault Tolerance (BFT) algorithms for reaching consensus on verifiable data [4], the challenge of achieving consensus on subjective or non-deterministic matters within DAOs [5] remains a complex issue [6][7]. This has led some researchers to question the ability of autonomous organizations to overcome the hierarchical issues present in today’s society [8][9].

This paper introduces a novel protocol designed to bridge the gap between formally verifiable, automated consensus and subjective human decision-making. By qualifying participants based on their

ability to represent a group’s interests and intents, our protocol aims to achieve consensus even for subjective matters. This protocol serves as a foundational building block for designing ranking systems applicable to both computational and social networks, addressing long-standing governance issues such as agenda manipulation [10].

The main objectives of this research are to:

- Propose a methodology for creating a ranking system in a trustless environment
- Review potential attack vectors and resistance mechanisms.
- Provide a case study of an existing use case.
- Discuss potential economic models for the practical utilization of such competence frameworks.

We begin by reviewing existing consensus mechanisms and their limitations, focusing on DAOs and their governance mechanisms. We then introduce our proposed protocol, followed by a discussion of its implementation and potential economic models. Finally, we present a case study of an existing use case and conclude with a discussion of future research directions.

2 Background

Decentralized Autonomous Organization governance acts software program that formulates social agree-

ment of how management occurs within some group of independent agents. Consensus engines of popular today blockchains implement such formulation for a very application-specific goal. Due to subjective reasoning of agents, DAOs cannot be defined completely through cyber-physical systems [11] methodology, which aims to define how cyber system may operate physical systems at scale. Nevertheless, an end goal for any autonomous governance is to operate CPS, which might evolve in future far enough to fully automate management of manufacturing plants, data centers and other cyber-physical infrastructure key components. In order to accommodate for that, Fei-Yue et.al proposed that any kind of IT governance system can be seen through methodology of Cyber-Physical-Social-System (CPSS) [12] which attempts to account for social aspect of intellectual management, including specifics of post-AI age where Artificial generic Intellect is real.

Parallel management concept is introduced recently by same researchers using CPSS to specifically address management perspectives in cyber age [13]. This work actualizes importance of highly efficient and autonomous decision making and feedback processes. Such framework requires DAOs as core element of such CPSS. The need for multidimensional indices as well as foundational models for measuring knowledge works is also discussed [14]. References to DAOs as instrument within CPSS and parallel management means there is a need to ensure, that such a dependency is well architected to provision future breakthroughs and enables efficient management processes that do not risk becoming a performance bottleneck. The needs for parallel management don't stop on that, a robust mechanism for reinforcing the informational and intellectual capabilities of organizations, enabling them effectively create knowledge works and benchmark performance of AI and other agents in various tasks and aspects of governance and management is discussed [13].

Nakamoto Coefficient. Since cryptographic decentralization emerging as industry additional metrics are needed to measure quality and performance indicators for such organizations. Nakamoto Coefficient is a recently introduced concept that helps to measure decentralization of a protocol [15]. It is defined as *how many entities one would need to to be compromised to control entire system* and it can be used as decentralization criteria.

Traditional governance models While this is not a focus of our research at this point, we can point out that traditional governance have unresolved problems, widely known and yet not addressed. Particular one is agenda manipulation problem, [10] which is something to take in account when game theoretic moments become in play. Another prominent issue are participation rates (turnout), which also being studied and seen to be in decline in major countries over past decades [16][17].

2.1 Consensus Layer

Before discussing a consensus seeking means within DAOs, let's first review the underlying blockchain models and their consensus means and challenges. Blockchain technology, also known as Distributed Ledger Technology today, in principle, is a set of rules of how the chain of linked records is stored and modified within a distributed database that is hosted by potentially malfunctioning operators. Such ledger book record follows some particular consensus protocol in order to maintain continuous sequence, chain of blocks[18], where each new block consists of a digital records to a united ledger book. First introduced at launch of Bitcoin[3], since then grown to an industry where multiple approaches and protocols were developed and initial ability to write a records in to ledger book was elaborated to ability to write code in ledger records such that can change states of book itself.

The blockchain governance plays a critical role in such a protocol which can in high level be described as consisting of separate participant kinds: Validators, Users, Governance Mechanisms and core developer community; In this context DLT is analogous to an organization, consisting validators (employees), protocols and governance structure whose activity result in services provided to users that also have to say their word by paying for using the protocol.

The contrast between traditional organization and blockchain governance is CSP friendly automation. If a cyber system runs such a DLT instance, it can immediately use records as source of operational directives. Such directives in their turn may be designed to follow predetermined rules of maintaining distributed ledger with no need for human stakeholder decision, fully automating operations. Such consensus based decision making systems, however, work only well up to the point when the protocol changes are desired or some vulnerability happens which leads to stakeholder collective decision

for stepping-off the protocol rules for at least one block[19]. Such occasions happen casually when community agrees to change rules of the protocol. Popular name for such event in DLT protocol is "hard-fork" which underscores split of consensus in two possible ledger book states: before and after the introduced change.

MEV: Consensus protocols have the underlying node operator community which was shown to be strongly incentive driven, studies on Nash Equilibrium by Nida Khan et.al [20] show possible fragility of such community. Real situation for Ethereum was analyzed by Philip Daian et.al., results have shown that Miner Extracted Value (MEV) poses as realistic threat to protocol level security that comes down to affecting applications such as decentralized exchanges[21]. Same paper also observes that agents pursuing MEV can achieve cooperative equilibrium in terms of priority gas auctions.

Participation and Decentralization Dominic Grandjean et.al. has shown that practical Nakamoto coefficient numbers in automated consensus engines such as PoS and Pow (Proof of Stake and Work accordingly) have stabilized on a very low numbers of less than 5 entities capable of quorum, and seem not to show any positive dynamics [22].

2.2 Application Layer

By application layer we mean using ability to create programs within DLT records, a concept pioneered by V.Buterin in Ethereum protocol. Such governance mechanisms, coined as DAOs, have a distinct property difference from consensus layer discussed previously. By relying on the automated consensus rules of generic ledger book, these systems are able to optimize and allow subjective, decentralized discussion conversion resulting a decision making on the DLT. While research in CPSS field point out demand for such DAOs as a solution [12][13][14], the ability of DAOs to perform well and be competitive, however, is under question, as many researchers point out associated problems [7][8][9].

Nakamoto coefficient. An empirical Study of On-Chain Governance conducted by Rainer Feichtinger et. al. [7] shows low Nakamoto coefficient numbers, however comparing it with Consensus Layer research

[22] we can conclude there is a positive dynamic in the Nakamoto coefficient over time in DAOs, compared with absence of such for the consensus layer.

Turnout. Same research[7] also shown that analyzed DAOs Gini coefficients[23] are high, reaching 0.888-1 for direct holders and 0.667-0.980 range when counting delegates. This indicates participation rate in DAOs are low.

Out of four analyzed DAOs (Compound, Uniswap, ENS and Gitcoin), none of them are showing positive dynamics in participation rate over time, and mean numbers for participation even amongst delegates are in range of 1.1-9.9% of total delegated accounts.

Centralization problems are shown by Robin Fritsch et.al at [24], which concludes that two analyzed DAOs, namely Compound and Uniswap DeFi protocols in fact are extremely centralized and controlled by a very small number of addresses, while their governance systems are looking more like a board director meetings, where a small number of large investors represents actual governing power. Such research indeed questions whether such organization really can be fully seen as autonomous and decentralized.

Quorum thresholds & efficiency is another highlighted problem. Since blockchain DAO data is public, it is easy to analyze. For example, Compound DAO quorum requires only 400,000 [25] votes out of 10,000,000 total token supply [26], which is only 4%, yet in practice some of proposals fail to reach even this low threshold from the first time and have to re-submit [27][28]. To illustrate problem further quorum requirements of few high value DAOs are illustrated in Table 1. Ethereum PoS validator count is also shown to represent a consensus level engine specifics. Such low quorum requirements are directly explainable by a low participation rates. A record of quorum attacks precedents showing resulting security weakness [29][30].

2.3 Comparing two above

Contrary to application layer, we've seen high participation rate consensus layer systems, such as PoS and PoW, the financial incentives towards participation shown not just to negatively impact Nakamoto coefficients, but also have shown that any network

Table 1: DAO Minimal Quorums

Name of DAO	Total Supply	Quorum	Threshold (%)
Compound	10e6	400e3	4%
Uniswap	1e9	40e6	4%
ENS	100e6	1e6	1%
Arbitrum	10e9	300e6-500e6	3-5%
Lido	1e9	50e6	5%
Ethereum PoS	120e6 (33e6 staked)	22e6 (66% of 33e6)	19%

node must be seen as rational-agent which may diverge from collective interest [21], yet even with that, the technical complexity and network requirements result in only 19% effective quorum attack threshold for whole Ethereum L1 at the time of writing.

DAOs ultimately are just an abstraction layer on top of Consensus, allowing blockchain users to abstract away from calculations intensity onto smart contract programming and therefore more versatile, dynamic governance systems that can rely on underlying consensus security guarantees. Hence, while Consensus layers do provide participation incentives, the application layer organization might not propose such at all, instead providing a framework for taking a governance decisions that may bring incomes on their own.

Comparing Nakamoto coefficients we can see a notable difference between the two layers, referenced papers show different slopes. One possible explanation for this phenomenon can be coined as "curse of money making money". It suggests that in order to ensure growth of Nakamoto coefficient, the ability to influence the system should grow at a rate that must be sub-linear in relation to ones efforts, ensuring that no disproportionate compounding of power occurs. In other words, the growth of influence should not match nor exceed a linear rate to prevent centralization, highlighting the necessity for mechanisms that enforce a diminishing increase in influence relative to investment or contribution (Fig. ??).

One another notable difference is in the security model. While relying on consensus engine enables security guarantees, the opposite side of that medal is that such application layer governance mechanisms have no similar alternative as consensus layer operators do with hard-fork ability. Even if community members agree on such decision in case exploit happens, there is no easy way to "split away" saving full state. The only known occasion of such successful

split was The DAO Hack Hard-fork which was done very controversially at the protocol level. [19]. This is a substantial difference with consensus layers, where any participation requires a commitment that either requires to do work prior to a particular vote (PoW), or have assets at stake (PoS, Optimistic Rollups) that can be lost during due to any activity by operator against the protocol rules.

Lack of such ongoing commitment mechanisms in the application layer, brings in substantial security risks as governance attacks become less risky for the adversary [29][30]. Such risks led to solutions such as time-locks [31], and rage quit [32] methods giving individual stakeholders a last-resort options to leave the protocol (arguably) safely at the expense of delayed actions taken by the organizations.

While these solutions are effective in preventing funds loss, the reduce in reaction time by organization is not always acceptable. Need for prompt decision making is leads to empowering security players to run a privileged multi-signature wallets to run emergency stop or veto power over DAO protocols [33]. Fact of presence of such, centralizing actors makes DAO frameworks to behave in non-autonomous way. The more general question is left open - how to appoint such privileged actions takers in an autonomous ways, ideally defining the privileges as a function of certainty in the actor?

2.4 Recent cryptographic advancements

Recent cryptographic advancements have enabled the development of new governance and consensus mechanisms that may be used to address the challenges faced by DAOs. For example, the use of zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) allows for the creation of verifiable and private voting systems that can be used to ensure the integrity of voting processes within DAOs [34], while MPC threshold-signature protocols can be used to

create secure multi-party data signing process [35] and fully homomorphic encryption promises us soon ability to run fully private calculation directly on-chain [36].

Summing this section up, we can say that whatever new protocol is designed for governance, it is realistic to set requirements of privacy in voting and proposing process.

2.5 Proposed Protocol origins

The foundation of this research stems from a game played by a small group of Lithuanian friends in a chat messenger since 2017. Initially designed for leisure and sharing music, this game has unexpectedly exhibited properties desirable in governance protocols.

The game, played by 5 to 10 participants, involves a rotating "game master" role. Each round, participants submit music they enjoy to the game master, who compiles them into a playlist. Participants then vote on their favorite composition, and the game master reveals the results, including proposer identities and scores. The game continues until 100 compositions are added to the playlist, with the final ranking based on accumulated scores[37].

This game's design inherently resists agenda setter manipulation due to its mandatory proposal-submission prerequisite for voting, a stark contrast to traditional voting systems vulnerable to small-group dominance[10]. Furthermore, it effectively mitigates negative proposal effects like the Halo effect [38].

Interestingly, the game demonstrates high participation and retention rates, suggesting potential for adaptation as a governance protocol (elaborated in case study section). The primary limitation lies in participants' inclination towards specific interests (music in this case) or groups of people.

The game's communication complexity appears to be $O(3n)$ per round, as participants submit a proposal, receive a batch of proposals, and then submit a vote.

This research aims to build upon this foundation, exploring the game's potential as a scalable, decentralized governance protocol with built-in resistance to manipulation and high participant engagement.

2.6 Summing up the context

From the issues identified in the background sections we can sum up that there are multiple problems

that are faced both on network protocol level governance as well as on application layer built DAOs: Low participation rates, low Nakamoto coefficients (high centralization), lack of application layer commitments, inability to perform time-critical actions autonomously and in decentralized fashion, lack of multidimensional indices needed for knowledge work assesement.

We can also see that incentive based protocols cause centralization when using own governance power equivalent as reward for protocol participation, yet decentralized organizations are not able to provide a commitment mechanism for participants, nor do they have truly autonomous way to appoint stakeholders purely from the mission it has, nor identify competent actors in the system to take prompt, time-critical actions.

Both on consensus layer based on continuous proving and application layer with share-holder voting we identified different problems. To some extend these problems are generic, and explained by lack of ability to autonomously distribute governance power, the recent studies have shown that Initial Coin Offerings (ICOs) are very susceptible to speculations and might be seen as root cause centralization [39]. This leads to situation where reputable security and venture capital funds suggest new players a "progressive decentralization" approach to coupe with the threats[40][41], yet these articles do not offer a sustainable and scalable mechanism for decentralizing and staying efficient. We also outlined that already existing DAO precedent can show positive dynamics in Nakamoto coefficient when influence is sub-linear to efforts (or completely absent), compared to Consensus Layer systems that incentivize participants. We also outlined precedent of a game that has high participation rates and user retention (further elaborated in case study section).

3 Protocol Description

In order to enable deductive reasoning, we can outline specifications that a generic abstract organization must fulfill. Besides these, we preferably want to system to be compatible with existing solutions and technologies that allow data integrity, privacy and security, assuming that distributed ledger and multiparty computation signing may be combined to cover these problems.

We are seeking for protocol that is:

Mission aligned: Organization members should ac-

tively participate in the decision-making process by the design of the protocol, their activity shall be directly impacting the organization goals and mission.

Highly performant: Ideally, every organization design shall automatically align participants in collaborative model, enabling everyone to do their best contribution towards shared direction, with utilizing full potential of competitive performance provided by decentralized autonomous methodology.

Centralization resilient: Protocol should be designed in a way that over time dependency on single actors shall be reduced, Nakamoto coefficient shall increase, promoting collaboration over competition for those aligned in automatic manner.

Multidimensionality: Protocol should enable multidimensional indexes and foundational models to be built on top of it, as well as promote working groups that can be more operative than a main governing body. At the global scale this should support automatically combining multiple DAOs in superset and enable establishing data, asset and control specific flows-controls.

Rational: Protocol should be designed in a way that any network node must be seen as rational-agent which may diverge from collective interest or collude with others and still not able to reach influence over the system beyond what protocol accounts for.

In order to define quantitative metrics over these declared values in a most generic way, we will use vector space modelling. Such social embedding is used to refer to the representation of individuals or groups as vectors within a social network. Let's introduce the concept of a agent alignment vector, denoted as \vec{A} . This vector captures the collective preference of the group that can be seen as united entity within a given context, such as publicly announced topic, or any other group member specific property. We can denote such context as global alignment vector as:

$$\vec{G} = \sum_{i=0}^{N_i} \vec{A}_i + \vec{C} \quad (1)$$

Where N_i denotes total number of such groups at given time and \vec{C} is some predefined context constant value. If we assume numerous such possible contexts denoted N_j , then we also can denote an universal alignment vector describing every possible context j as:

$$\vec{U} = \sum_{j=0}^{N_j} \vec{G}_j \quad (2)$$

To define a performance criteria, we can denote time dependency for these vectors, to underscore their ever changing nature of decision making:

$$U(\vec{t}) = \sum_{j=0}^{N_j} G_j(\vec{t}) = \sum_{j=0}^{N_j} \left(\sum_{i=0}^{N_i} A_{ij}(\vec{t}) + \vec{C}_j \right) \quad (3)$$

In such case, a prompt decision making process, describing ability for high performance can be seen as derivate function of time:

$$\frac{d\vec{U}}{dt} = \sum_{j=0}^{N_j} \frac{d\vec{G}_j}{dt} = \sum_{j=0}^{N_j} \left(\sum_{i=0}^{N_i} \frac{dA_{ij}}{dt} + \vec{C}_j \right) \quad (4)$$

Deducting of our requirements, the mission alignment is can be seen as stability of $\vec{U}(t)$ and $\vec{G}_j(t)$ over time, multidimensionality is quantified by N_j , participation rates by N_i while centralization by standard deviation of the magnitudes of a set of vectors $\vec{A}_{ij}(t)$ and can be denoted as follows:

$$\sigma_{\|\vec{A}_{ij}(t)\|} = \sqrt{\frac{1}{N_i N_j} \sum_{j=0}^{N_j} \sum_{i=0}^{N_i} \left(\|\vec{A}_{ij}(t)\| - \mu \right)^2} \quad (5)$$

where $\|\vec{A}_{ij}(t)\|$ represents the magnitude of the vector $\vec{A}_{ij}(t)$, and μ is the mean magnitude of the vectors, given by:

$$\mu = \frac{1}{N_i N_j} \sum_{j=0}^{N_j} \sum_{i=0}^{N_i} \|\vec{A}_{ij}(t)\| \quad (6)$$

Assuming that \vec{A} represents groups interest, it can be further broken down as the aggregate of individual preference vectors \mathbf{P}_i . In such, a group ideal delegate can be defined as a participant whose \mathbf{P}_i aligns most closely with \vec{A} . This alignment maximizes their positive contribution to the overall group preference and can be quantified using measures like cosine similarity or Euclidean distance between the participant's and the group's vectors.

Such "ideal" candidate obviously inherits some rounding error:

$$\cos(\theta) = \frac{\vec{A} \cdot \vec{P}_i}{\|\vec{A}\| \|\vec{P}_i\|} \quad (7)$$

In the ideal scenario, the group would just have weights according to theirs score values, however, in real world, as previously stated in requirements, the group needs to be able to take decisions in high-performant manner, hence the ideal candidate is the

one that can make decisions on behalf, and in the best interest of the group, in the most efficient way. This is where the concept of a ranking ladder comes into play, which we will discuss in the next section.

The protocol’s inclusive and autonomous requirement nature allows to envision that even a fully stochastic process, where participants could be assumed to make random decisions regarding tournament participation, proposals, and voting, an \vec{A} could be defined. However, we postulate the existence of an underlying, unknown global alignment vector $\mathbf{G}(\mathbf{t})$, that reflects the overall preferences of all protocol participants across time.

This concept accommodates the diverse preferences of all participants, even in the boundary case of entirely random decisions. In this fully stochastic scenario, the group’s alignment is characterized by entropy, a measure of randomness. The Euclidean distance of each member’s rank from the most probable rank for a random participant can serve as a measure of their capacity for random decision-making.

Conversely, in non-stochastic processes, participants exhibit alignment towards an arbitrary direction, shaped by their free-will choices to join specific groups and context. The protocol goals hence can be seen as to quantify these vectors and ensure their desired properties.

3.1 Transferability

In order to support solving all of the objectives, we propose to specify, that outcome of protocol is a transferrable asset, that can effectively tokenize the competence rating of bearer. Transferability is an important aspect as this allows free market rules to establish and accomplish multiple goals, starting with agent rational actions: even concepts of corruption and collusion can be seen as game-theoretic [42], are not necessarily bad [43], and can be seen through definition of an intrinsic value of any transferable asset. Other words saying, we see personal competences in CPSS frameworks useful as a market value, that may be useful to trade.

While this can be argued as a controversial statement, we can discuss that in the real world competence indeed is often traded in form of a investing time and money in education, relationships, that eventually form a social ranking. Since we declare as a requirement to have a compounding resistance, it forms a solid basis for building economic models that penalize competence-market participants heavy enough, so that competence is not traded in a way that it can be easily bought by a single entity. Trans-

ferability of value opens vast application opportunities, as other protocols are free to define staking commitments with specific slashing rules, similarly as PoS consensus mechanisms do, therefore bringing one of the lacking consensus layer features on-to on-chain governance. Eventually, this helps forming a rational economic model that would incentivize any participant to treat his rating in a similar careful and responsible manner, as one does with his assets.

With such, we envision that both \vec{A} and \vec{G} may be tokenized separately, whilst there is connection between these, reciprocity is not a strict requirement, meaning that while conversion of \vec{A} into \vec{G} must be supported by protocol as per Eq. 1, the reverse exchange can be left for a free market to decide upon, leaving some extra space for protocol incentives design which we will use in following sections to create additional useful properties for the protocol. Nevertheless, transferability does not exclude any applications where such rating asset must be locked. Use cases of ownership within Account Abstraction[44] model could be designed to ensure asset is non-transferable and acts as account-bond proof of competence if such an use case would be desired.

Token economics, and their application in governance systems are widely used today, however mechanisms such as Initial Coin Offerings (ICOs) have shown to be a weak spot as this opens doors for bad entrepreneurs [39], and as already discussed in background section, ultimate outcome of such allocation is extremely centralized, and suspect of issues such as centralization and inability to perform well.

3.2 Continuous voting-proposing

In order to accommodate for rounding error produced in Eq. 7, we propose to inherit from original protocol described in 2.5 the continuous voting-proposing system. This continuous process enables to agents to train their alignment, reducing overall entropy of the group, and hence increasing the overall alignment vector \vec{G} discovery process. The continuous nature of the protocol allows for the alignment vector to be updated in real-time, reflecting the most recent preferences of the group as well as it enables for winning \mathbf{P}_i that is chosen as groups delegate to change over time, therefore the the rounding error produced by Eq. 7 can be time averaged across participants. Ranking ladder proposed in next section would also improve this process, as the most aligned delegates will be incentivized to switch their group to a higher ranked one, hence allowing group to find next most aligned delegate in a more efficient way.

3.3 Ranking ladder

Providing a resistance to influence compounding becomes a critical aspect part for such protocol, since we are relying to a free-market values and principally do not require any specific identity solution as a dependency to this protocol. Our foundational model for this resistance lies in extending 2.5 idea, to introduce *ranking ladder* (Fig. 3) that lets game winner to participate in next game with higher level of rewards only if it holds an asset of rank below. Such architecture allows to design initially low ability to influence \vec{G} and exponentially increase as participant succeeds climbing up ladder. As participants gain higher ability to influence global alignment value, quantitative measure of that is their individual preference vector magnitude $|P|$, which protocol accounts for increasing only as they prove to be the most impactful part of their group $|A_i|$.

Participant rank R hence represents such quantization of $|A_i|$:

$$R = Q(|A_i|) \quad (8)$$

To further introduce compounding resistance, we define protocol ladder climb event requirement: previous ladder step tokenized element must be removed (exchanged) in order to derive next rank, resulting a simple ladder that can be seen as kind of tournament system.

In order to see how this affects protocol parameters on practice, we can analyze a collision attack scenario, which is one of most prominent threads for any permissions less protocol that produces intrinsic value.

If each game requires a commitment, such as a participation fee, we can demonstrate that the proposed ranking ladder introduces a desired non-linear compounding friction for potential malicious actors attempting to manipulate the system.

To illustrate this, let's use the concept of a agent alignment vector introduced in Eq.(1). In the absence of collusion or manipulation, a blind proposing-voting process is inherently probabilistic, where the inverse of groups magnitude $|\vec{A}|$ quantifies the resistance to entropy inherent in every participants' natural choices.

Any colluding actors attempting a Sybil attack are effectively trying to manipulate global alignment vector $\mathbf{G}(\mathbf{t})$ by becoming a delegate of $|\vec{A}_i|$ portion of it. Given our earlier requirements for an ideal protocol, it should encourage the formation of small groups

while maintaining a large overall active participant count. This can be implemented as breakdown into smaller groups, which serves as a pre-alignment mechanism, as participants willingly choose to collaborate. Similarly, additional requirements can be imposed on the participants by group creators, such as humanity checks. Various different protocols can be used such as Proof of Location[45] or proof of personhood[46]. Outside of this group context, any group can be seen as already to some extent colluding, with Sybil attacks representing an extreme case of such alignment. Therefore our proposal is for autonomous competence rating is to declare by design, that *colluding groups are allowed, and that the protocol is designed to resist such attacks*.

Therefore, from the outset, each group is inherently aligned towards a specific direction, determined by the free will of its members to participate in a particular tournament. This pre-alignment introduces a degree of predictability, quantified by $|\vec{A}|$, into an otherwise stochastic process.

If there is a fee, that creates participation resistance (financial, and hence energetic), we can say that achieving a specific level of competence cost is $\$R$ and can be expressed as a function of level of competence i and game fee X_g with mathematical expectation for costs achieving specific rank via sybil attack described as

$$\mathbb{E}[\$R] = X_g \cdot \mathbb{E}[N_{\text{sybils}}(R)] \quad (9)$$

Where $N_{\text{sybils}}(R)$ is a number of sybil accounts required to win a game, and hence obtain rank R . Due to tournament fragmentation, an attacker mixing Sybil accounts with fair players must strategically allocate Sybils across games for cost efficiency. However, this is challenging due to each group's unique \vec{A} , finding suitable games for manipulation is difficult. Meanwhile, from a deductive reasoning, the distance between fair actors' preferences P_i and $\mathbf{G}(\mathbf{t})$ should diminish as their rank increases, reflecting the protocol's design of identifying participants alignment.

This means that for any protocol participant, confidence over group conducting a sybil attack will increase as level of games increase, hence they will be more likely to refuse joining games with such, resulting

$$\lim_{R \rightarrow \infty} \frac{\mathbb{E}[N_{\text{sybils}}(R)]}{R} = N_{\min} \quad (10)$$

Where N_{\min} is amount of peers required to join the game. Hence, a straightforward Sybil attack scenario where the attacker attempts to manipulate the protocol by flooding games with multiple Sybil accounts

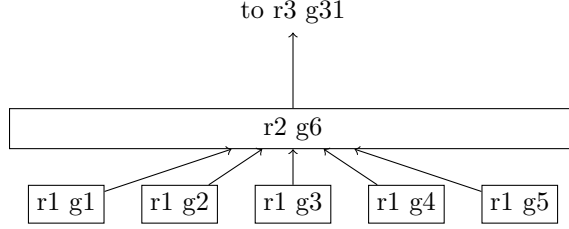


Figure 3: Diagram illustrating the rank ladder. With minimum participant requirements of 5, 30 games are required to create a rank 3 game. Strong candidate would need only 2 wins to reach it.

may be analyzed. Then for an attacker who tries to conduct a sybil attack it would cost

$$\$R = X_g * N_{min}^R \quad (11)$$

to get rank of level i . At the same time, for the agent who is relying on his pure competence and wins each game, same cost would be only

$$\$R = X_g * R \quad (12)$$

In the context of governance power, this allows to draw price relationship between governing competence power that may be put at stake, and total value locked (TVL) at stake:

$$TVL \ll \$R \quad (13)$$

Total value locked must be substantially lower then a cost for obtaining rank due to reason that empirical studies are needed to see how fast will required sybil count converge (Eq. 10) in practice. which strongly depends on how much stochastic process is inherit in such voting system. Additionally sybil resistance will benefit greatly from use of quadratic voting systems which already shown to be helpful in blockchain governance field [47][48].

3.4 Time constraint

As discussed in the previous section, any overt Sybil attack requires multiple game rounds to establish a sufficient ranking within the system. In the original protocol, participants engage in several voting and proposing rounds to determine a winner.

We preserve this multi-round requirement to enhance protocol security, ensuring resistance to centralization and maintaining mission alignment. We introduce a time constraint, t_c which represents the minimum time needed to mint a single competence asset of any rank. Therefore, the intrinsic value of a tokenized competence rating is determined not

only by financial effort and success among peers but also by the time invested in continuously improving one's position within the system. Even with parallel attack instances, an attacker would still require $t_{attack}(R) = t_c \cdot R$ time to reach rank R . This extended duration allows protocol members ample opportunity to detect and respond to the attack. Similarly, the t_c may be broken down to smaller components, giving participants ability to leave or cancel a game, specify round times etc.

3.5 Composable architecture

The DAO hack[19] a single entity governing on-chain operations creates a central point of failure. Even with a theoretically perfect design, a single governing body struggles to match the versatility, adaptability of smaller groups is desired [49]. This highlights the necessity of multidimensionality to achieve a robust, global DAO concept while maintaining high performance. Furthermore, the time constraints discussed in Section 3.4 imply that changes in \vec{G}_j (Eq.4) should be gradual, even under ideal conditions. To address these challenges, we propose a composable architecture where each potential \vec{G}_j operates as an independent DAO. This eliminates single points of failure and enables the parallel emergence of successful solutions.

A non-permissive rating system, tokenized via rating representation R , empowers competent participants by amplifying voting power or granting specific permissions within an organization or contract. The global, distributed DAO \vec{U} , emerges as the aggregate of all G , representing a theoretical value not elaborated upon in this work.

Participants gain subject-specific competence R_j , which determines governance weights (W_j) within the corresponding DAO: $W_j = f(R_j)$. As $R_j = f(t_c)$ (time-dependent), resulting weights are also time-dependent: $W_j = f(t_c)$. The protocol facilitates the transformation of R_j into W_j .

From Eq. 1 and Eq. 8 it is possible to infer that

protocol must provide means of transforming to such DAO governance weights W_j . This has been already discussed in Sec. 3.1 that such conversion does not require to be reciprocal, meaning that reverse conversion may be market defined. This is a useful property as multiple financial and market instruments may be designed to ensure stimulus for participants to pursue their success strategy within the protocol.

Exit Strategies and Governance Transitions.

Existing DAO frameworks can leverage fungible tokens derived from R_j through a unidirectional asset exchange. This enables high-scoring participants to "exit" and convert their competence into governance power within the underlying DAO, essentially forming a specialized "guild" (Fig. 4). While the rating asset R holds intrinsic value, high-scoring participants may stagnate at the top due to a lack of competition. Additionally, tokenized ratings are better suited for reputation representation than direct governance, as they are vulnerable to unforeseen losses during possible third party staking. The exchange into governance weight W_j symbolizes a transition from service provision (risking reputation) to a managerial role, where participants focus on generating intrinsic value for the DAO.

Exponential Rewards and Sybil Attack Mitigation. To incentivize participation and prevent stagnation, exponential rewards are necessary, especially for higher ranks with fewer participants. Governance power must also account for potential sybil attacks:

$$W_{gj}(R) \propto X_{gj} * \mathbb{E}[N_{sybils_j}]^{R_j} \quad (14)$$

Where $\mathbb{E}[N_{sybils_j}]$ is expectation of required N_{sybils} . If a group of high-scoring participants exits, they're likely to gain substantial power in the underlying DAO, whose reputation is established from past rounds. This aligned group effectively represents $G_j(t)$ at a specific time when they achieve quorum.

DAO Dynamics and Evolution. The original protocol competence generation algorithm stay unaffected and already established uses for competence rating system with asset of R are unaffected by the new governance power distribution of W_j . However, the new DAO quorum can define $G_j(t)$ for their specific subset and control the organization's public descriptions and URIs. This incentivizes the new DAO

to increase its market value, justifying the exit strategy and driving demand for the X_g asset needed for W_j .

The Nakamoto coefficient increases over time as new participants enter and gain power. Early adopters can maintain control by strategically acquiring lower-ranking members' R_j , creating a reverse market that balances R to W_j . Active participation is crucial for maintaining power in the face of inflation and new entrants.

Composable DAO Framework and Network Effects.

A composable DAO framework emerges when a high-scoring group deploys another autonomous competence protocol with a subsidiary DAO, linking both to a shared asset holding contract such as new multisignature wallet. This effectively splits the organization, with asset ownership tied to the original but governance shared between the two bodies. The derived protocol cost can be linked to the parent DAO (\dot{X}_{gj} to G_j), forming a network of interconnected DAOs (Fig. 5).

This architecture offers a decentralized, scalable, and adaptable governance model, incentivizing participation and excellence while mitigating centralized control and stagnation risks.

3.6 Privacy constraints

This paper addresses privacy requirements in a proposal evaluation protocol. The protocol aims to balance transparency and anonymity by:

- **Linking Proposals to Proposers:** Enabling the association of proposal submissions events with specific proposers, without revealing the proposal content initially.
- **Verifying Proposal Uniqueness:** Ensuring the submitted proposal was uniquely known to the proposer at the time of announcement, while preserving proposer anonymity.
- **Protecting Preference Selection:** Safeguarding the privacy of participant preferences during proposal selection.

These measures aim to mitigate the Halo effect [38], where judgments are influenced by personalities rather than ideas, and deter strategic voting by increasing the complexity of coordinated attacks against competent proposals. The de-personalized voting process aims to foster a fairer evaluation environment by focusing on the merit of the proposals

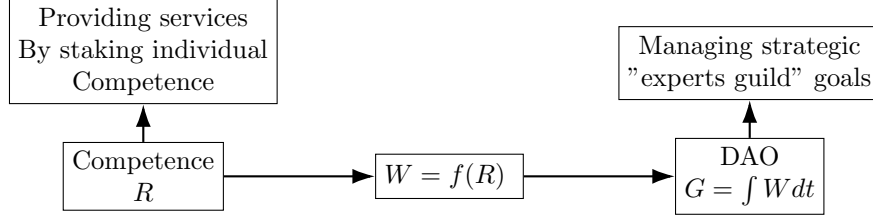


Figure 4: Competence transfer to DAO voting weights

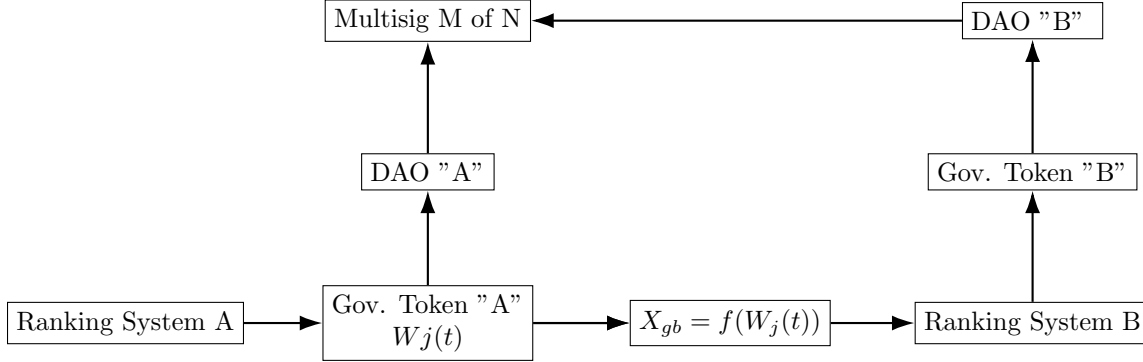


Figure 5: Diagram describing progressive decentralization via DAO composition. As initial group governing DAO "A" experiences inflation it may provision next organization "B" to focus on specific aspects of arbitrary protocol, and maintain any asset security by moving them further on to the governance chain. If such assets are assigned to multisig, original DAO value is preserved, therefore allowing organization to grow both horizontally and vertically.

themselves.

4 Implementation

Protocol particular implementation may vary depending on environment and requirements, however we can outline a generic implementation that can be used as a reference for further development. Following reference describes implementation as a smart contract on Ethereum Virtual Machine compatible network.

Rating asset is semi-fungible tokenized asset contract, such as defined by ERC1155[50] interface standard and with emission permit granted only to contract(or contracts), that implements autonomous rating identification. Participation fee X_g is expressed as ERC20[51] token interface which may represent a overseeing organization governance power. Privileged methods available to rating identification contracts: minting new token, burning existing token from owners balance.

Competence identifaciton contract operates by logic that is given in (Algorithm ??). The specific rules of produced by autonomous decision making based on competence identification goals, may be specific for goals. For example, if goal is to formulate one, finalized proposal over multiple round, a later rounds based proposals could be seen as more refined and hence applied higher weights.

DAO, Governance Token & Multisig can be used from already established frameworks for token based voting may be used. Various frameworks for DAOs are available[52][53], as well as industry standard multisignature wallet[54]. In standard implementation we suggest requiring 2/3 quorum threshold on the multisignature wallet.

Game Master concept is needed to provide privacy. The game master is responsible for collecting proposals and announcing fact of activity without disclosing the actor, then posting them as batch to a competence identification contract, collecting votes in a similar manner, without tell nor who, nor for whom votes, and finally revealing the results.

This is potential failure point as such agent may disclose or even attempt to corrupt data. Whilst in our

simple implementation a trusted backend server is used, an ideal solution can be achieved by multiparty computation, where every participant seen as network participant that can sign transactions with encrypted data, and decrypt it according to the protocol requirements. Fully on-chain fully-homomorphic encryption promised by emerging blockchains poses interest[36].

5 Case Study

5.1 Original Concept: A Music-Sharing Game

To gather empirical data, we analyzed a group’s activity and historical records in a music-sharing game [37]. Participants share YouTube music clips, forming playlists. From 2017 to 2023, 17 games were played, each averaging 13 turns, 8 participants, and 3 months duration. Roughly 1700 proposals and votes were recorded, with a 100-song playlist limit per game. Over the years, 34 participants joined, 22 completing at least one tournament and 15 completing at least two. Of the original 6 players, 3 remain active, with 8 active users in the latest game. Non-voting instances were negligible, below 5% of all votes. Despite lacking explicit incentives and requiring effort as occasional game masters, participation rates were remarkably high:

- **Participation rate** of 95% for active users
- **User retention** for three month period of 65%
- **User retention** for two tournaments and roughly six month of 44%
- **User retention** after 72 month of 9%
- Average of **8 proposals and votes per user** per annum

The low absolute numbers however are explainable by user complex manual score calculation process and closed community by itself which never oriented itself towards big growth and hence let to do assertion that could be even higher on a well designed automated protocol.

We also observed that collected playlists, ordered by high-score compositions, are of high quality and form a good representation of participants’ preferences, while the winner of the tournament is often a participant that is able not simply propose a popular song, but to propose a song that is liked by many participants, including such aspects that participants will likely vote songs they hear for the first time (orig-

inal ideas).

5.2 Prototype study

We wrote a simple implementation of such game that allows ease game process with game automation. Two games were conducted each game consisted of 9 participants. Participants included original concept participants and random people who did not know each other of different age groups. Game rules and requirements were set close to original: participants were required to send URLs for music on youtube with composition length of no more than 10 minutes and had to listen for all of them in order to make a vote. Privacy constraints were ensured by a backend server. Quadratic voting system was used, allowing users to spend 14 vote credits in integer form. Only notable difference was that for sake of design simplification, the total playlist length was replaced with fixed round count.

Participants were given no incentives, and most of the group had no prior blockchain experience nor significant interest in it.

Some participation rate metrics were recorded during these two games:

- **Participation rate** of 84% for active users
- **User retention** of 66.7% after first game
- Average of **3.23 proposals and 3.09 votes per user** per month

Based on conducted experience, participants were asked to fill feedback form, questions asked was possible to rate from 0 to 5.

- **Overall experience rating:** 88%.
- **Resulting playlists rating:** 92%.
- *“Did playing this game give you new insights into the personalities or perspectives of other players?”*: was rated at 80%.
- *“Would you be willing to play such game with your friends or family?”*: was rated at 84%.

Out from participants that left game could be noted significant age, and preference difference Participants also proposed various different game topics and generally expressed interest.

When asked *“If you missed any turn to vote or propose, what were main causes”*, all respondents answered that they enjoyed the process however lacked time to listen all of the compositions.

6 Potential Applications

Better ICOs: By releasing an ERC20 token as payment for competence games, projects can create a more meritocratic system where participants earn governance tokens based on their demonstrated skills and contributions. This approach aligns incentives, rewards active engagement, and fosters a community of competent stakeholders who are genuinely invested in the project's success.

Autonomous Code-Writing: In software development, the autonomous competence identification protocol can revolutionize the code-writing process. By treating each round as a programming cycle, developers can submit pull requests, vote on the best solutions, and iteratively refine the codebase. The fixed cycle length ensures a strict deadline, promoting efficiency and focus. The protocol's ability to weight later rounds more heavily acknowledges the cumulative improvement of code over time, incentivizing continuous participation and innovation. Participants are encouraged to actively contribute new code and solutions rather than just reviewing and commenting, fostering a proactive and collaborative development environment.

Cross-Stream Collaborative Integrations: Continuous opinion exchange nature of the protocol can be used to create a seamless platform for cross-stream collaboration and feedback gathering. This reduces the need for time-consuming meetings and calls, enabling teams to collaborate more efficiently and effectively. By fostering a culture of continuous feedback and iterative improvement, the protocol can enhance communication, streamline decision-making, and drive innovation across various streams within an organization.

Decentralized Social Networks: the protocol could assess the quality and relevance of user-generated content, such as posts, comments, and shares. By assigning higher rankings to valuable contributions, the protocol can incentivize users to create meaningful content and discourage spam or low-effort posts. Additionally, it can help identify influential users based on their consistent engagement and the quality of their interactions, fostering a more meritocratic and engaging social media environment.

Academic Research and Peer Review: The traditional peer-review process often suffers from biases, delays, and lack of transparency. The autonomous competence identification protocol can address these issues by creating a decentralized peer-review system. Researchers can submit their work, review others' submissions, and receive ratings based on the quality and thoroughness of their reviews. This approach can lead to faster, more objective, and transparent peer review, ultimately improving the quality and credibility of academic research.

Online Education and Skill Assessment: The protocol can be applied to online education platforms to assess and certify learners' skills. By participating in competence games or challenges, learners can demonstrate their knowledge and proficiency in various subjects. The protocol's ranking system can provide a verifiable and transparent way to assess skills, enabling learners to showcase their expertise to potential employers or educational institutions.

Prediction Markets: The autonomous competence identification protocol can enhance these markets by identifying participants with a proven track record of accurate predictions. By assigning higher weights to their forecasts, the protocol can improve the overall accuracy and reliability of the market's predictions. Additionally, it can incentivize participants to continuously improve their forecasting skills to earn higher rewards.

Decentralized Autonomous Organizations : DAOs can utilize the autonomous competence identification protocol beyond governance to enhance various internal processes. For instance, the protocol can be employed to allocate resources efficiently by identifying members with the most relevant expertise and experience for specific tasks or projects. This ensures that resources are directed towards individuals who are most likely to utilize them effectively, maximizing the DAO's overall productivity and impact.

Furthermore, the protocol can be used to assign tasks within the DAO by matching members' skills and interests with the requirements of different roles or responsibilities. This can lead to a more motivated and engaged workforce, as members are more likely to excel in tasks that align with their strengths and passions.

Additionally, the protocol can be instrumental in evaluating proposals for new projects or initiatives

within the DAO. By assessing the competence and track record of the proposers, as well as the potential impact and feasibility of their ideas, the DAO can make more informed decisions about which projects to pursue, increasing the likelihood of success and minimizing risks.

Empathic Agenda and AI Applications: protocol establishes a framework for rating both participants and ideas, decoupling evaluation from personal biases. Its continuous feedback loop, utilizing previous round results, fosters deeper alignment among participants and cultivates empathy as they iteratively refine their understanding of collective preferences.

Beyond interpersonal empathy, this property holds significant value for Cyber-Physical-Social Systems (CPSS). By benchmarking AI agents participating in these games, the protocol generates feedback and historical data that can be used to create robust, personalized machine learning frameworks.

7 Conclusion

This paper has presented a novel protocol for establishing ranking systems in DAOs and consensus-building protocols, aiming to address challenges such as low participation, centralization, and lack of commitment mechanisms. By incorporating a competence-based approach, tokenized ratings, and a composable architecture, the protocol fosters a more engaging, equitable, and secure decision-making process. The real-world case study demonstrates the potential of this approach to drive high participation and retention rates, even without explicit incentives.

Future research could explore the development of more sophisticated economic models and incentive structures to further enhance participation and mitigate risks. Additionally, the protocol’s applicability could be investigated in various domains beyond music sharing, such as decentralized finance, social networks, and scientific collaboration. By bridging the gap between formal consensus mechanisms and subjective human decision-making, this research contributes to the ongoing development of more effective and inclusive governance models for the digital age.

References

- [1] X. Li, T. J. Andersen, and C. A. Hallin, “A zhong-yong perspective on balancing the top-down and bottom-up processes in strategy-making,” *Cross Cultural and Strategic Management*, vol. 26(3), 2019.
- [2] F. Vervaeke, *The High Command in the Roman Republic: The Principle of the Summum Imperium Auspiciumque from 509 to 19 BCE*. Historia, 2014.
- [3] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.
- [4] G. ZHANG and et. al, “Reaching consensus in the byzantine empire: A comprehensive review of bft consensus algorithms,” *arXiv*, vol. 03181v3, no. 2204, 2023.
- [5] S. Hassan and P. De Filippi, “Decentralized autonomous organization,” *Internet policy review*, vol. 10, no. 2, 20 April 2021.
- [6] S. Wang and et. al, “Decentralized autonomous organizations: Concept, model, and applications,” *IEEE TRANSACTIONS ON COMPUTATIONAL SOCIAL SYSTEMS*, vol. 6, no. 5, 2019.
- [7] R. Feichtinger, R. Fritsch, Y. Vonlanthen, and R. Wattenhofer, “The hidden shortcomings of (d)aos – an empirical study of on-chain governance,” *arXiv*, vol. 12125v2, no. 2302, Feb 2023.
- [8] M. Atzori, “Blockchain technology and decentralized governance: Is the state still necessary?,” *Available at SSRN: <https://ssrn.com/abstract=2709713> or <http://dx.doi.org/10.2139/ssrn.2709713>*, 2016.
- [9] X. Liu, “The illusion of democracy— why voting in decentralized autonomous organizations is doomed to fail,” *NYU Law and Economics Research Paper*, vol. 13, no. 24, 2024.
- [10] R. D. McKelvey, “Intransitivities in multidimensional voting models and some implications for agenda control,” *Journal of Economic Theory*, vol. 12, no. 3, 1976.
- [11] E. A. Lee, “Cyber physical systems: Design challenges,” in *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, pp. 363–369, 2008.
- [12] F.-Y. Wang, M. Xiao Wang, L. Li, and L. Li, “Steps toward parallel intelligence,” *IEEE/CAA JOURNAL OF AUTOMATICA SINICA*, vol. 3, no. 4, 2016.
- [13] W. Fei-Yue, “Parallel management: The dao to smart ecological technology for complexity management intelligence,” *ACTA AUTOMATICA SINICA*, vol. 48, no. 11, 2022.
- [14] J. Li, R. Qin, and F.-Y. Wang, “The future of management: Dao to smart organizations and intelligent operations,” *IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS*, vol. 53, no. 6, 2023.
- [15] B. S. S. et al., “Quantifying decentralization.” <https://news.earn.com/quantifying-decentralization-e39db233c28e>, 2017 [Accessed Jun. 2024].
- [16] L. Ezrow and W. Krause2, “Voter turnout decline and party responsiveness,” *British Journal of Political Science*, vol. 85–103, no. 53, 2023.
- [17] F. Kostelka, S. P. Singh, and A. Blais, “Is compulsory voting a solution to low and declining turnout? cross-national evidence since 1945,” *Political Science Research and Methods*, vol. 76–93, no. 12, 2024.
- [18] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, and A. Peacock, “Blockchain technology in the energy sector: A systematic review of challenges and opportunities,” *Renewable and Sustainable Energy Reviews*, vol. 100, pp. 143–174, 2019.
- [19] L. Liu, S. Zhou, H. Huang, and Z. Zheng, “From technology to society: An overview of blockchain-based dao,” *IEEE Open Journal of the Computer Society*, vol. 2, pp. 204–215, 2021.

- [20] N. Khan, T. Ahmad, A. Patel, and R. State, “Blockchain governance: An overview and prediction of optimal strategies using nash equilibrium,” *arXiv:2003.09241 [cs.GT]*, 2020.
- [21] P. Daian, S. Goldfeder, T. Kell, Y. Li, and X. Zhao, “Flash boys 2.0: Frontrunning, transaction re-ordering, and consensus instability in decentralized exchanges,” *arXiv*, vol. 05234v1, no. 1904, 2019.
- [22] D. Grandjean, L. Heimbach, and R. Wattenhofer, “Ethereum proof-of-stake consensus layer: Participation and decentralization,” *arXiv*, vol. 10777 [cs.DC], no. 2306, 2023 [Accessed Jun. 2024].
- [23] L. Ceriani and P. Verme, “The origins of the gini index: extracts from variabilit  e mutabilit  (1912) by corrado gini,” *The Journal of Economic Inequality*, vol. 3, no. 10, 2012.
- [24] R. Fritsch, M. M uller, and R. Wattenhofer, “Analyzing voting power in decentralized governance: Who controls daos?,” *arXiv preprint arXiv:2204.01176*, no. 2204.01176v1, 2022.
- [25] “Compound dao contract.” Ethereum Network: 0xc0Da02939E1441F497fd74F78cE7Decb17B66529.
- [26] “Compound token.” Ethereum Network: 0xc00e94Cb662C3520282E6f5717214004A7f26888.
- [27] Tally, “Compound dao proposal 232 voting page.” <https://www.tally.xyz/gov/compound/proposal/232>, 2024.
- [28] Tally, “Compound dao proposal 237 voting page.” <https://www.tally.xyz/gov/compound/proposal/237>, 2024.
- [29] A. Association, “Aragon association takes action to safeguard the mission of the aragon project and its community of builders.” Web archive: <https://web.archive.org/web/20240228120235/https://blog.aragon.org/aragon-repurposes-dao-to-ensure-treasury-serves-its-mission/>, 2023.
- [30] rhizoo.eth, “The rook dao story: Postmortem of the \$25m governance takeover.” <https://www.bitget.com/news/detail/12560603820648>, 2023.
- [31] J. CURATOLO, “Protect your users with smart contract timelocks,” *OpenZeppelin Blog*: <https://blog.openzeppelin.com/protect-your-users-with-smart-contract-timelocks>, 2021.
- [32] A. Soleimani, A. Bhuptani, L. H. James Young, and R. Sethuram, “The moloch dao: Beating the tragedy of the commons using decentralized autonomous organizations,” <https://raw.githubusercontent.com/MolochVentures/Whitepaper/master/Whitepaper.pdf>, 2019.
- [33] J. Scharfinan, “Decentralized autonomous organization (dao) fraud, hacks, and controversies,” *The Cryptocurrency and Digital Asset Fraud Casebook*, vol. 2, 2024.
- [34] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, “Scalable zero knowledge via cycles of elliptic curves.” Cryptology ePrint Archive, Paper 2014/595, 2014. <https://eprint.iacr.org/2014/595>.
- [35] J. Doerner, Y. Kondi, E. Lee, and abhi shelat, “Threshold ecdsa in three rounds,” *IEEE S P*, 2023.
- [36] G. Zyskind, Y. Erez, T. Langer, I. Grossman, and L. Bondarevsky, “The-rollups: Scaling confidential smart contracts on ethereum and beyond,” 2023.
- [37] D. Treinys, “Youtube playlists, music challenges.” <https://www.youtube.com/@dariustreinys8150/search?query=challenge>.
- [38] B. Verhulst, M. Lodge, and H. Lavine, “The attractiveness halo: Why some candidates are perceived more favorably than others..” <https://doi.org/10.1007/s10919-009-0084-z>, 2010.
- [39] J. Fuchs and P. P. Momtaz, “Token governance in initial coin offerings: Implications of token retention and resale restrictions for ico success,” *Small Bus Econ*, 2024.
- [40] J. Walden, “Progressive decentralization: A playbook for building crypto applications.” (<https://a16z.com/progressive-decentralization-a-playbook-for-building-crypto-applications/>).

- [41] S. Webber, “How web3 progressively decentralizes using openzeppelin governor.” (<https://blog.openzeppelin.com/how-web3-progressively-decentralizes-using-openzeppelin-governor>).
- [42] J. Macrae, “Underdevelopment and the economics of corruption: A game theory approach,” *World Development*, vol. 10, no. 8, 1982.
- [43] N. H. Leff, “Economic development through bureaucratic corruption,” *American Behavioral Scientist*, vol. 3, no. 8, 1964.
- [44] Q. Wang and S. Chen, “Account abstraction, analysed,” *arXiv [cs.CR]*, no. 2309.00448, 2023.
- [45] P. Sheng, V. Sevani, R. Rana, H. Tyagi, and P. Viswanath, “Bft-poloc: A byzantine fortified trigonometric proof of location protocol using internet delays,” 2024.
- [46] WorldCoin, “Private by design.” (<https://worldcoin.org/privatebydesign-whitepaper>).
- [47] V. Buterin, Z. Hitzig, and E. G. Weyl, “A flexible design for funding public goods,” *Management Science*, vol. 65(11):5171–5187, 2019.
- [48] A. Benhaim, B. H. Falk, and G. Tsoukalas, “Balancing power in decentralized governance: Quadratic voting and information aggregation,” 2024.
- [49] V. Buterin, “Daos are not corporations: where decentralization in autonomous organizations matters,” <https://web.archive.org/web/20240327003454/https://vitalik.eth.limo/general/2022/09/20/daos.html>, 2022, accessed on 22 jul 2024.
- [50] W. Radomski, A. Cooke, P. Castonguay, J. Therien, E. Binet, and R. Sandford, “Erc-1155: Multi token standard.” <https://eips.ethereum.org/EIPS/eip-1155>, 2018. Accessed: 2024-10-04.
- [51] F. Vogelsteller and V. Buterin, “Erc-20: Token standard.” <https://eips.ethereum.org/EIPS/eip-20>, 2015. Accessed: 2024-10-04.
- [52] A. Association, “Aragon osx dao framework.” (<https://github.com/aragon/osx>).
- [53] OpenZeppelin, “Governor dao framework.” (<https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/governance/Governor.sol>).
- [54] G. Safe, “Safe smart account.” (<https://github.com/safe-global/safe-smart-account>).