# Autonomous competence identification protocol

Tim Pechersky

July 25, 2024

**Abstract**

This paper proposes a novel protocol for designing ranking systems applicable to consensus-building protocols and decentralized autonomous organizations (DAOs). Leveraging recent cryptographic advancements and social science insights, the protocol facilitates autonomous decision-making in trustless environments based on agent interactions, addressing key challenges in autonomous organizations. We examine an existing precedent, originating as an easy-to-understand tabletop game, which demonstrates promising participation rates even among non-technical users. Our proposed implementations focus on defining interoperable and liquid voting weights for participants, facilitated in both computational and non-computational (social) networks. Additionally, we briefly review economic models for the practical utilization of such competence frameworks and game theoretic moments.

## 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 addresses the gap between formally verifiable, automated consensus and subjective human decision-making. We propose a protocol that can achieve consensus even for subjective matters by qualifying participants based on their ability to represent a group's interests and intents. This protocol aims to provide a foundational building block for designing ranking systems applicable to both computational and social networks, and capable to address some of long standing governance issues such as agenda manipulation [10] problem.

Main objectives thus are to propose a methodology for creating a ranking system in a trustless environment, review attack vectors and resistance mechanisms, provide a case study of existing use-case and 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 governance nor consensus protocols cannot be defined completely trough cyber-physical systems [11] methodology. Nevertheless, an end goal for any autonomous governance is to operate CPS. In this context any kind of IT governance system can be seen trough methodology of Cyber-

Physical-Social-System (CPSS) [12].

Studies of management perspectives in cyber age introduce parallel management [13] ideas, management frameworks proposed to model DAOs as CPSS openly discuss need for multidimensional indexes and foundational models [14]. In order to support such grand design ambition, the DAO organizations must be able to show other metrics of their governance to provide the best possible performance. Additionally, as discussion for parallel management [13], there is a need for a robust mechanism for reinforcing the informational and intellectual capabilities of organizations, enabling them effectively benchmark performance of AI enabled agents against human in various tasks and aspects of governance and management.

In order to support quantities analysis of decentralization metric, Nakamoto Coefficient[15] was proposed, defined as *how many entities one would need to to be compromised to control entire system* it can be used as decentralization criteria.

Besides these new concepts, the traditional governance models long standing problems, such as agenda manipulation [10] that should be addressed well to ensure high reliability of organizations in autonomous systems.

## 2.1 Consensus Layer

Blockchain is a distributed and decentralized network that follows some particular consensus protocol in order to maintain continuous sequence, chain of blocks[16], 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 any blockchain protocol and can be summarized as consisting of Validators, Users, Governance Mechanisms and core developer community; In this context blockchain network 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. Such are designed to follow some determined rules of maintaining distributed ledger with no need for human stakeholder decision for a regular operations which are automated by running specific software applications (nodes) that act on behalf of stakeholder. These 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 [17] for at least one block. Such occasions generally are called hard-forks and have specifics that coordinated consensus between node operators changes their protocol rules to move away from existing logic. The "fork" in context describes split of consensus in two possible ledger book states which are not compatible.
Consensus layer protocols also have the underlying node operator community which incentive driven and studies on Nash Equilibrium [18] are done while the real situation for Ethereum is that Miner Extracted Value is shown [19] as realistic thread to protocol level security that comes down to affecting applications such as decentralized exchanges. Same paper also observes that agents pursuing MEV can achieve cooperative equilibrium in terms of priority gas auctions.
"Ethereum Proof-of-Stake Consensus Layer: Participation and Decentralization research" [20] 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 then 5 entities standing behind whole pool of validators and miners, and seem not to show any positive dynamics.

## 2.2 Application Layer

While research in CPSS field point out demand for DAOs as 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].
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 [20] 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. Same research[7] also shown that analyzed DAOs Gini coefficients[21] are high, reaching 0.888-1 for direct holders and 0.667-0.980 range when counting delegates, also shown participation rate in DAOs are low. Out of four analyzed DAOs (Compound, Uniswap, ENS and Gitcoin), none of them are showing positive dynamics in

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% |

participation rate over time, and mean numbers for participation even amongst delegates are in range of 1.1-9.9% of total delegated accounts.

Another highlighted problem can be seen in the voting participation quorum thresholds, which are low. For example, Compound DAO quorum requires only 400,000 [22] votes out of 10,00,000 total token supply [23], 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 [24][25]. 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, and already have a record of quorum attacks [26][27] precedents, that were exploiting this weakness, while contrary in 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 node must be seen as rational-agent which may diverge from collective interest [19], 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.

## 2.3 Comparing two above

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. Difference however also lies in implementation specifics: while Consensus layers do provide participation incentives, the application layer organization might not propose such at all, instead providing a means to make a governance decisions that are profitable on their own.
Analyzing Nakamoto coefficient we can see a notable difference between Nakamoto coefficient in DAOs vs Consensus layer. 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 entities efforts (investments), 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. [17]. 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 [26][27]. Such risks led to solutions such as time-locks [28], and rage quit [29] 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 [30]. 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 [31], while MPC threshold-signature protocols can be used to create secure multi-party data signing process [32] and fully homomorphic encryption promises us soon ability to run fully private calculation directly on-chain [33].
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[34].
This game's design inherently resists agenda 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 [35].
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 as well: Low participation rates, low Nakamoto coefficients, lack of application layer commitments, and lack of multidimensionality. We can also note that incentive based protocols cause centralization, 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.
We have discussed two different kinds of systems so far - based on consensus layer continuous proving and application layer share-holder voting and identified different problems of both of these kinds. We also outlined that already existing DAO precedent can show positive dynamics in Nakamoto coefficient when influence is sub-linear to efforts, 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 actively 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, 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:

$$\vec{G} = \sum_{i=0}^{N_i} \vec{A_i} + \vec{C} \tag{1}$$

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:

$$\vec{U} = \sum_{j=0}^{N_j} \vec{G_j} \tag{2}$$

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

$$\vec{U(t)} = \sum_{j=0}^{N_j} \vec{G_j(t)} = \sum_{j=0}^{N_j} (\sum_{i=0}^{N_i} \vec{A_{ij}(t)} + \vec{C_j}) \tag{3}$$

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

$$\frac{d\vec{U}}{dt} = \sum_{j=0}^{N_j} \frac{d\vec{G_j}}{dt} = \sum_{j=0}^{N_j} (\sum_{i=0}^{N_i} \frac{d\vec{A_{ij}}}{dt} + \vec{C_j}) \tag{4}$$

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:

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

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

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

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.

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 $\mathbf{G(t)}$,

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 [36], are not necessarily bad [37], and can be seen trough 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. Transferability 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[38] 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.

### 3.2 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 will account 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 $|A_i|$:

$$R = Q(|A_i|) \tag{7}$$

To further introduce compounding resistance, we define protocol ladder climb event requirement: previous ladder step tokenized element must be removed (exchanged) in order to obtain higher ladder rank.

In order to see how this affects protocol parameters on practice, we can analyze a sybil 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

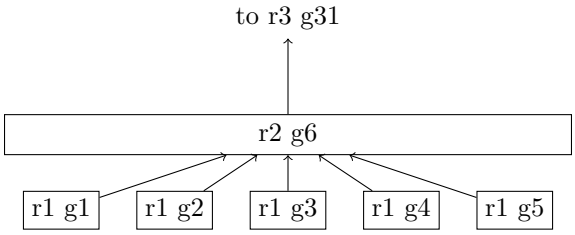


Figure 3: Diagram illustrating the rank ladder. With minimum participant requirements of 5, 30 games are required to create a rank 3 game. Strong candidate would need only 2 wins to reach it.

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 participants' choices.

Any colluding actors attempting a Sybil attack are effectively trying to manipulate this global alignment vector $\mathbf{G}(\mathbf{t})$. 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 breakdown into smaller groups serves as a pre-alignment mechanism, as participants willingly choose to collaborate. In this context, any group can be seen as colluding, with Sybil attacks representing an extreme case of such alignment.

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 game fee, that creates participation resistance, 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 $X_g$ and mathematical expectation for costs achieving specific rank via sybil attack described as

$$\mathbb{E}[\$R] = X_g \cdot \mathbb{E}[N_{\text{sybils}}(R)] \tag{8}$$

Where $N_{sybils}(R)$ 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

$$\lim_{R\to\infty} \frac{\mathbb{E}[N_{\text{sybils}}(R)]}{R} = N_{\min} \tag{9}$$

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

$$\$R = X_g * N_{min}^R \tag{10}$$

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

$$\$R = X_g * R \tag{11}$$

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 loked (TVL) at stake:

$$TVL << \$R \tag{12}$$

## 3.3 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.

### 3.4 Composable architecture

The DAO hack[17] 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 [39]. This highlights the necessity of multidimensionality to achieve a robust, global DAO concept while maintaining high performance. Furthermore, the time constraints discussed in Section 3.3 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. 7 it is possible to infer that protocol must provide means of transforming to such DAO governance weights $W_j$. This 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:

$$W_{gj}(R) \propto X_{g_j} * \mathbb{E}[N_{sybils_j}]^{R_j} \tag{13}$$

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

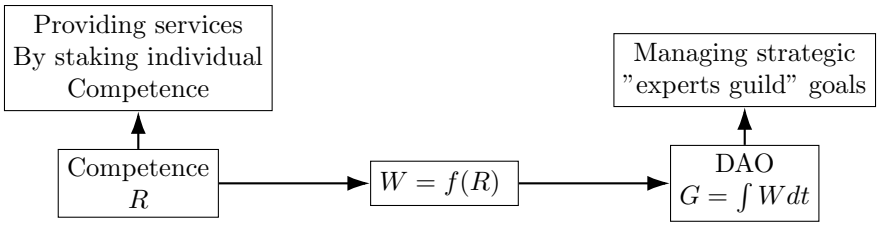


Figure 4: Competence transfer to DAO voting weights

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. TThis 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 ($\grave{X}_{gj}$ 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.

### 3.5 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 [35], 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 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[40] 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[41] 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 1). 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.

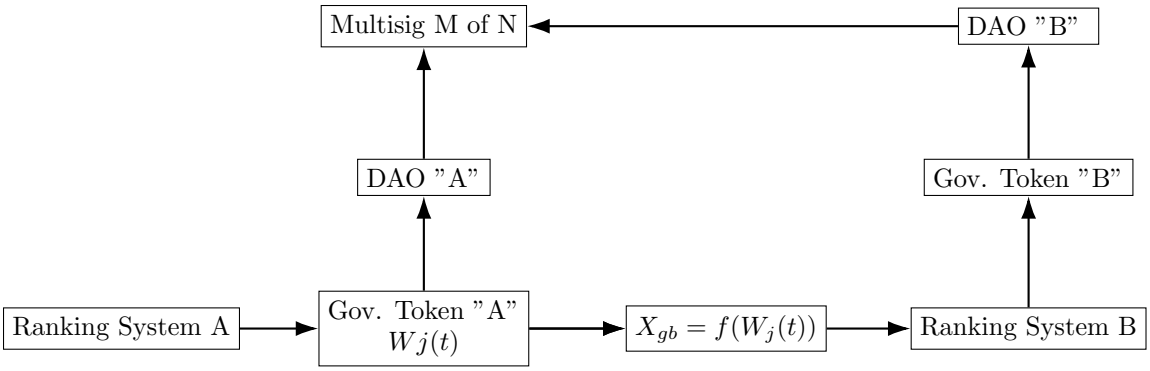


Figure 5: Diagram describing progressive decentralization via DAO composition. As initial group governing DAO "A" experiences inflation it may provision next organization "B" to focus on specific aspects of arbitrary protocol, and maintain any asset security by moving them further on to the governance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

**DAO, Governance Token & Multisig** can be used from already established frameworks for token based voting may be used. Various frameworks for DAOs are available[42][43], as well as industry standard multisignature wallet[44]. In standard implementation we suggest requiring 2/3 quorum threshold on the multisignature wallet.

**Game Master** 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.
Multi-party computation, network the initial "Game Master" is potential failure point as he may disclose or even attempt to corrupt data. Ideal solution can be achieved by multiparty computation, where every participant runs a network that can sign transactions with encrypted data, and decrypt it. Fully on-chain fully-homomorphic encryption promised by emerging blockchains poses interest[33]. In our most simple implementation a trusted server is used as privacy proxy.

# 5 Case Study: A Music-Sharing Game

To gather empirical data, we analyzed a group's activity and historical records in a music-sharing game [34]. 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 participant** 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 (original ideas).

# 6 Conclusion

In this paper, we have explored the implementation and empirical analysis of a music-sharing game within a decentralized autonomous organization (DAO) framework. Our study demonstrates that high participation rates and user retention can be achieved even without explicit incentives, highlighting the potential for community-driven engagement in decentralized systems.

We have shown that the competence of participants can be effectively measured and utilized to drive decision-making processes within DAOs. By leveraging historical data and user interactions, we can create a robust mechanism for governance that aligns with the collective interests of the community.

Furthermore, our findings suggest that integrating such competence-based protocols can enhance the scalability and security of DAOs. This approach not only mitigates the risks associated with Sybil attacks but also ensures that decisions are made by qualified participants, thereby fostering a more resilient and trustworthy governance model.

As DAOs continue to evolve, the need for sophisticated governance mechanisms becomes increasingly critical. Our proposed methodology offers a promising direction for future research and development, aiming to bridge the gap between automated protocols and human-centric decision-making processes.

In conclusion, the integration of competence-based consensus mechanisms within DAOs presents a viable path towards more effective and decentralized governance. By harnessing the collective intelligence and active participation of community members, we can build more robust and adaptive decentralized organizations capable of addressing complex challenges in a trustless environment.

# A Appendix A: Listings

**Algorithm 1** Basic Autonomous competence identification

**Prerequisites:** Minimal group size $N_{min}$, Time constant $t_c$, Participation cost $X_g$, Competence Asset $C_i$, Protocol Treasury $T$, Minimal turn count $M, M > 2$
**Process:**
**procedure** PREPARATION
    Instance is created at timestamp $t_0 = t$, with creators personal join requirements $X_a$
    Participants join the group and lock in a commitment: $N_{min} \times (X_g + X_a) \to T$
    Joining period ends at $t_1 \geq t_c + t_0$
**end procedure**
**procedure** FIRSTTURN
    **while** $t_1 + t_c \geq t$ **do**
        **if** new Proposal **then**
            Record $P_i$
            Record $i$
        **end if**
    **end while**
    **if** Group is full or joining timeout **then**
        Members exchange encrypted proposals (MPC).
    **end if**
**end procedure**
**procedure** DECRYPTPROPOSALS
    **if** Timeout or all proposals received **then**
        Members decrypt proposals using threshold encryption.
    **end if**
**end procedure**
**procedure** REGULARTURN
    Submit new encrypted proposals.
    Submit encrypted votes and zk-proof of valid vote.
**end procedure**
**procedure** CALCULATEROUNDSCORES
    **if** Round ends or all votes & proposals submitted **then**
        Use TSS cryptography to decrypt everything.
        Calculate round scores.
    **end if**
**end procedure**
**procedure** REPEATUNTILXPROPOSALS
    Repeat steps 3-5 until a total of X proposals.
**end procedure**
**procedure** FINALIZERANKINGS
    Count total votes and sort proposals.
**end procedure**

# 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. Vervaet, *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-decentalization-e39db233c28e, 2017 [Accessed Jun. 2024].

[16] 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.

[17] 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.

[18] 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.

[19] P. Daian, S. Goldfeder, T. Kell, Y. Li, and X. Zhao, "Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges," *arXiv*, vol. 05234v1, no. 1904, 2019.

[20] 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].

[21] L. Ceriani and P. Verme, "The origins of the gini index: extracts from variabilita e mutabilita (1912) by corrado gini," *The Journal of Economic Inequality*, vol. 3, no. 10, 2012.

[22] "Compound dao contract." Ethereum Network: 0xc0Da02939E1441F497fd74F78cE7Decb17B66529.

[23] "Compound token." Ethereum Network: 0xc00e94Cb662C3520282E6f5717214004A7f26888.

[24] Tally, "Compound dao proposal 232 voting page." https://www.tally.xyz/gov/compound/proposal/232, 2024.

[25] Tally, "Compound dao proposal 237 voting page." https://www.tally.xyz/gov/compound/proposal/237, 2024.

[26] 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.

[27] rhizoo.eth, "The rook dao story: Postmortem of the $25m governance takeover." https://www.bitget.com/news/detail/12560603820648, 2023.

[28] J. CURATOLO, "Protect your users with smart contract timelocks," *OpenZeppelin Blog: https://blog.openzeppelin.com/protect-your-users-with-smart-contract-timelocks*, 2021.

[29] 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.

[30] J. Scharfman, "Decentralized autonomous organization (dao) fraud, hacks, and controversies," *The Cryptocurrency and Digital Asset Fraud Casebook*, vol. 2, 2024.

[31] 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`.

[32] J. Doerner, Y. Kondi, E. Lee, and abhi shelat, "Threshold ecdsa in three rounds," *IEEE S&P*, 2023.

[33] G. Zyskind, Y. Erez, T. Langer, I. Grossman, and L. Bondarevsky, "Fhe-rollups: Scaling confidential smart contracts on ethereum and beyond," 2023.

[34] D. Treinys, "Youtube playlists, music challenges." `https://www.youtube.com/@dariustreinys8150/search?query=challenge`.

[35] 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.

[36] J. Macrae, "Underdevelopment and the economics of corruption: A game theory approach," *World Development*, vol. 10, no. 8, 1982.

[37] N. H. Leff, "Economic development through bureaucratic corruption," *American Behavioral Scientist*, vol. 3, no. 8, 1964.

[38] Q. Wang and S. Chen, "Account abstraction, analysed," *arXiv [cs.CR]*, no. 2309.00448, 2023.

[39] 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.

[40] 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.

[41] F. Vogelsteller and V. Buterin, "Erc-20: Token standard." `https://eips.ethereum.org/EIPS/eip-20`, 2015. Accessed: 2024-10-04.

[42] A. Association, "Aragon osx dao framework." (https://github.com/aragon/osx).

[43] OpenZeppelin, ""governor" dao framework." (https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/governance/Governor.sol).

[44] G. Safe, "Safe smart account." (https://github.com/safe-global/safe-smart-account).