

Autonomous competence identification protocol

Tim Pechersky

July 24, 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 through 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 through 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 threat 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:

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

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.

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 [36], are not necessarily bad [37], 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. 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 $|A_i|$:

$$R = Q(|A_i|) \quad (7)$$

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

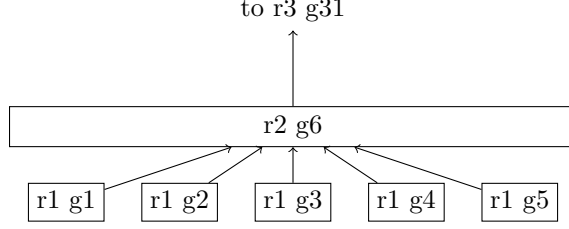


Figure 3: Diagram illustrating the rank ladder. With minimum participant requirements of 5, 30 games are required to create a rank 3 game. Strong candidate would need only 2 wins to reach it.

compounding friction for potential malicious actors attempting to manipulate the system.

To illustrate this, let's use the concept of an 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

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

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

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

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

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

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

$$\$R = X_g * R$$

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:

$$TVL \ll \$R$$

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

As evidenced by 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. Beside that, from time constraints introduced in Sect. 3.3 it can be deduced that speed of change in \vec{G}_j , described by Eq.4 even with best design thought in mind will, and should be a relatively slow process. This can be achieved by perceiving every possible \vec{G}_j as a separate DAO entity, eliminating single point of failure yet allowing successful and more effective solutions to emerge in parallel way.

With such in mind, a A non-permissive rating system, whose outcome is tokenized via rating representation R , can be used to compose an amplification of voting power or grant specific permissions within an arbitrary organization or contract to competent participants. A global, distributed DAO emerges as the sum of all G_j as \vec{U} , which may be seen as rather theoretically existing value which we won't elaborate further in this work right now.

keeping set of DAOs G in mind, protocol participants gain subject-specific competence R_j leading to a DAO with governance weights W_j defined solely by competence identification process: $W_j = f(R_j)$. Since by protocol design $R_j = f(t_c)$, of a specific member is always a property of time, the resulting weights are also function of time $W_j = f(t_c)$. From Eq. 1 and Eq. 7 it is possible to infer that protocol must provide means of transforming R_j 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.

Existing DAO frameworks using fungible tokens fit this model, as their governance token can be derived from R_j through a unidirectional asset exchange. Such asset separation creates an exit strategy for high-scoring participants, allowing them to reset their competence score in favor of governance power in the underlying DAO, which under assumption of specific subject elaborated, represents expert "guild" (Fig. ??). While the rating representing asset R is useful on it own and has an intrinsic value, the high-scoring participants eventually might form a small group of $N_{min}+1$ members who are above majority of protocol member rating, and hence might stale there, as there is no competition to grow within. Additionally, the tokenized rating R is envisioned to act as a reputation representation that is easy to stake due to it quantized intrinsic value, however this also makes it a not very good element for typical DAO governing power, which relies on ability to hold asset without losing it to any unforeseen incidents such as might happen due to agent mistake in staking his reputation on third party protocols. Hence, the exchange on to governance voting weight W_j is envisioned as form of transition of an agent from performing services by risking his reputation on to a managerial position, which allows one to leave rating space and instead join field of experts who are able to vote on DAO organization itself to conduct additional, intrinsic value.

Due to the diminishing number of participants at higher ranks, exponential rewards are necessary to prevent stagnation and incentivize participation. The governance power function must also consider sybil attacks: $W_{gj} = f(R_j)$ would have to be exponential to ensure proportional rewards with a straightforward sybil attack case:

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

If a group of high-scoring participants exits in such a way, they're likely to gain significant power in the underlying DAO, whose reputation is established from past rounds. Such group is likely to be aligned due to A_i definitions and in quorum case becomes a practical representation of $G_j(t)$ in DAO form at particular t when they have the quorum. We intentionally denote this as function of time as this would not stop the competence minting for other participants. This

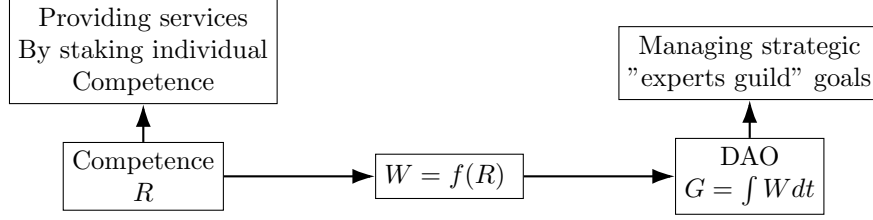


Figure 4: Competence transfer to DAO voting weights

action also would not affect already established possible uses for competence rating system with asset of R , as if such participant group would even be able to define $G_j(t)$ in favor of their specific subset A_i , they would not be able to affect in any means competence systems depending on $R_{i,j}$ due to unidirectional control flow with exception of the fact that these participants R_j value is zeroed in favor of DAO governance perspective, additionally, the ultimate power for organization could be to modify the context C defined in Eq.1, such could be descriptions and URIs of the organization that are publicly known to be property of G_j . This DAO managing group is incentivised to increase the market value of their exchanged governance power, justifying their exist strategy by generating additional intrinsic value, eventually driving demand on X_g asset required to receive W_j .

The Nakamoto coefficient in such a system increases over time as new participants may come in to the protocol and gain significant power as opposed to old-generation that took their exit at time they could have gained sufficient governance power. As the organization gains value, governance power inflation is expected yet is time delayed and can be forseen and couped by early holders. Early, high-ranking participants can maintain power by strategically purchasing lower-ranking members' R_j to prevent others from gaining higher ranks, which eventually forms a reverse market value, balancing R to W_j . Such governing DAO members however, must remain active to avoid being displaced by inflation and new participants.

A composable DAO framework emerges when a high-scoring group managing a DAO votes to deploy another autonomous competence protocol with a subsidiary DAO, adding both to a new multisignature wallet. This effectively splits the original organization, with asset ownership linked to the original but the Nakamoto coefficient accounting for both governing bodies. The derived protocol participation cost may be derived from parent DAO \tilde{X}_{gj} to G_j , creating a network of interconnected DAOs, Fig. 5.

This composable architecture offers a decentral-

ized, scalable, and adaptable governance model for DAOs. By incorporating competence-based governance and exponential rewards, it fosters a dynamic environment where participants are incentivized to contribute and excel, while mitigating the risks of centralized control and stagnation.

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, 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.

Concluding this section, we advocate that multi-dimensionality and free-market values will provide a way to ensure high participation rates, as participants will be able to participate in the decision-making process in a category that they are interested in, grouping with like-minded people in the fields

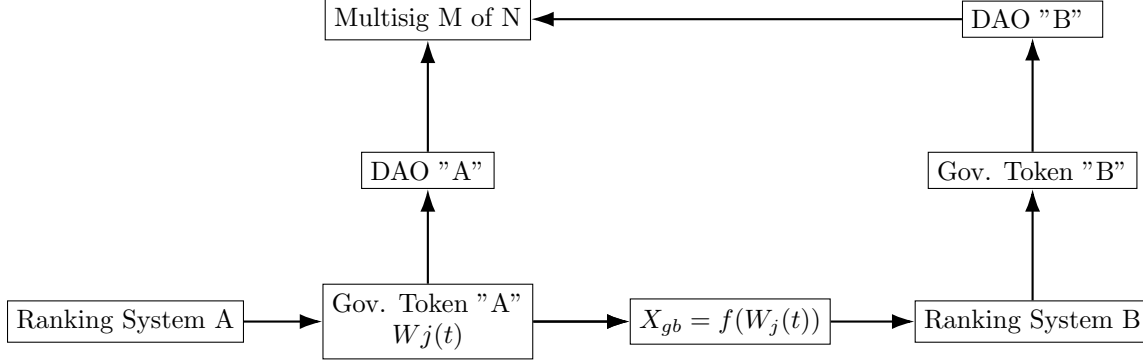


Figure 5: Diagram describing progressive decentralization via DAO composition. As initial group governing DAO "A" experiences inflation it may provision next organization "B" to focus on specific aspects of arbitrary protocol, and maintain any asset security by moving them further on to the governance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

they are competent in, and lastly - are rewarded for being in. With a ranking ladder, and a multidimensional representation, this can be seen as a global framework for building education and helping young talents to discover their path by observing very well quantized data on their progress.

We may also suggest that this protocol functionally may be presented as simply a new way of talking, where each input - seen as valuable idea, and each vote - seen as a valuable feedback, and each game final, as actionable result.

In order to support such high participation rates, the user experience must be ensured as simple as possible, and the application must be designed in a way that it is easy to use and understand. In order for that, we require to have extensive metadata available for user experience purpose by the protocol as key requirement. For example, when participant sends in

encrypted vote, or proposal - protocol shall be able to publicly announce that particular participant has submitted a vote, while not revealing the content of the vote nor the linkage to it after content is revealed for voting.

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.

Protocol consists of a semi-fungible tokenized asset contract, such as defined by ERC1155[40] interface standard and with emission permit granted only to contract or contracts, that implementing autonomous competence identification. Game participation fee for such contracts is pre-defined and may consist of arbitrary asset commitment. At this stage, protocol simply produces a competence representation in tokenized mean. The competence identification protocol contracts are turn-based continuous proposing-voting systems. Number of rounds and minimal time to make turns may be fixed to disavow any surprise governance attack. Game Master may be implemented as MPC network that obfuscated signs messages collectively

which will be either burned, either accumulated in DAO treasury DAO contract, any typical industry standard implementation may be used; An voting power token

that allows participants to submit proposals, vote on proposals, and receive rewards based on their participation. Subject representing subject asset can be represented as semi-fungible asset, like standard interface on Ethereum, where each token id represents a rank level, and games that award such rank require a token of one below to be held in order to participate.

Such tokenized asset shall be created (minted) only as a result of competence identifying smart contract activity result. The competence identifying contract

Algorithm 1 Basic Autonomous competence identification

```
1: Prerequisites: Minimal group size  $N_{min}$ , Time constant  $t_c$ , Participation cost  $X_g$ , Competence Asset  $C_i$ , Protocol Treasury  $T$ , Minimal turn count  $M, M > 2$ 
2: Process:
3: procedure PREPARATION
4:   Instance is created at timestamp  $t_0 = t$ , with creators personal join requirements  $X_a$ 
5:   Participants join the group and lock in a commitment:  $N_{min} \times (X_g + X_a) \rightarrow T$ 
6:   Joining period ends at  $t_1 \geq t_c + t_0$ 
7: end procedure
8: procedure FIRSTTURN
9:   while  $t_1 + t_c \geq t$  do
10:    if new Proposal then
11:      Record  $P_i$ 
12:      Record  $i$ 
13:    end if
14:  end while
15:  if Group is full or joining timeout then
16:    Members exchange encrypted proposals (MPC).
17:  end if
18: end procedure
19: procedure DECRYPTPROPOSALS
20:  if Timeout or all proposals received then
21:    Members decrypt proposals using threshold encryption.
22:  end if
23: end procedure
24: procedure REGULARTURN
25:  Submit new encrypted proposals.
26:  Submit encrypted votes and zk-proof of valid vote.
27: end procedure
28: procedure CALCULATEROUNDSCORES
29:  if Round ends or all votes & proposals submitted then
30:    Use TSS cryptography to decrypt everything.
31:    Calculate round scores.
32:  end if
33: end procedure
34: procedure REPEATUNTILXPROPOSALS
35:  Repeat steps 3-5 until a total of X proposals.
36: end procedure
37: procedure FINALIZERANKINGS
38:  Count total votes and sort proposals.
39: end procedure
```

is a turn-based game where group must collect together and has a signer-key (game master), who is able to sign for a private inputs and keep personalities of participants hidden by either using MPC or zk-SNARKs protocol. The game master is responsible for collecting proposals and announcing fact of activity without disclosing the actor, then posting them as batch to a contract, collecting votes in a similar manner, without tell nor who, nor for whom votes, and finally revealing the results.

5 Case Study

Some rough statistical data could be gathered by analyzing groups activity and historical records, which show that since 2017 total 17 games were played up to end of 2023. Each averaged for 13 turns, 8 participants and 3 month duration. Total amount of proposals and votes reaching 1700, as game is stopped at 100 songs playlist length. Total 34 participants joined it over course of years, out from which 22 players completed at least one full tournament and 15 completed at least two full tournaments. From original 6 players 3 still were playing at the moment of writing, with active user count 8 at latest game, showing steady with high user retention. Total amount of players not submitting a vote shown to be negligibly small, below 5% of all votes.

Even despite absence of any incentives beyond that participants are genuinely interested in the subject, and burden of having to be a game master occasionally which requires participants to do some effort, we can see exceptionally high user participation rates with average:

- 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).

5.1 Governance integration

In already established DAOs, this mechanism may be used to define slashing conditions. For example, a participant may have a right to perform privileged action on a DAO, by locking his competence level in escrow contract. If later, DAO votes with majority quorum condemning such an action as adversarial to the protocol, it may burn competence token of such an actor, which would result to have associated losses equal to cost of obtaining that competence asset. As per previous section, we've seen that such relationships may be reasoned.

For a broad and generic case, however, protocol use is envisioned to be able to bootstrap decentralized organizations, acting as replacement for initial-coin offerings [41] and airdrops popular in DAOs today. In this, a DAO bootstrapped by competence identification protocol creates own intrinsic value on the go, the long sustained participation with participation high participation rates may result in DAO led decisions to deploy infrastructure or elaborate any protocol that would embed intrinsic value to such.

This also seems like a very natural way for autonomous organizations to scale from security standpoint, as if any quorum, sybil attack and others

6 Conclusion

we are generalizing the proof based consensus mechanisms for social network interaction by viewing any network node as rational-agent which may diverge from collective interest [19] individually or collude with others. We propose BFT tolerance methodology that allows reaching effective consensus based on participant inputs, opinions and we can say that protocols reach an agreement in a trustless environment by qualifying the competence of the participants. Bitcoin miners are required to solve a cryptographic puzzle to prove their competence, or ethereum Proof of Stake consensus mechanism qualifies participants by

their ability by ability to adhere to distributed ledger rules and stake their assets.

Similarly DAO participants are qualified by their ability to hold a token and participate in the voting process. Tokens held can be seen as analogy to stake in PoS consensus mechanism, incentivising participants to act in the best interest of the organization. The gap however exists between such automated protocols and DAO governance as organizations agenda may be much more arguable than a "simple" cryptographic puzzle, which despite any computational complexity it might have, most of the time can be formally verified to be correct.

This becomes more emergent as the DAOs are becoming more complex and must take effective and prompt decisions in a trustless environment, which often leads to burden of complexity on users, while often a decision making process involves a fairly traditional board-level discussions within governance forum boards, which yields for doubts as researchers

find blockchain-based governance systems likely not to solve problems of social.

The contrast between traditional organization and blockchain is that latter are set to follow some determined protocol of following consensus layer decisions in an autonomous way, therefore enabling CPS, there is no need for human stakeholder decision for a regular operations which are automated by running specific software applications (nodes) that maintain protocol 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 need for stepping-off the protocol rules 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.

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] 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 re-ordering, 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. Scharfinan, “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, “The-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: 2023-10-04.
- [41] A. M.M., J. M., K. R.E., and et al., “Initial coin offerings: a hybrid empirical review,” *Small Bus Econ*, vol. 891–908, no. 61, 2022.