Autonomous competence identification protocol: A dynamic ranking ladder system for blockchain applications

Tim Pechersky, Aivars Smirnovs

December 14, 2024

Abstract

Meritocratic systems often struggle to identify and reward competence objectively. This paper proposes a novel protocol for establishing a dynamic ranking ladder system within trustless environments. By leveraging game-theoretic principles and dynamic systems theory, our protocol enables the autonomous identification of competence while mitigating potential sybil attacks. Participants engage in competitive "elections" within time-locked, tiered groups, with winners progressing to higher ranks. This process creates a quantifiable and verifiable measure of competence, represented by a tokenized rating. The protocol's time-based and cost-based mechanisms ensure that achieving high ranks requires genuine effort and skill, making it resistant to manipulation. Potential applications include merit based blockchain consensus, decentralized social networks, DAO governance.

1 Introduction

Traditional meritocratic models often falter due to the inherent difficulty of objectively identifying and rewarding competence.[1] This challenge is amplified in decentralized systems, where trust is minimized and the potential for manipulation is high. Existing consensus mechanisms, such as Proof-of-Work and Proof-of-Stake, may only proof that participant has either computational or financial power, but not necessarily competence needed, for example, to govern the protocol development. This hinders ability of decentralized systems developers to create robust governance and funding mechanisms that would be not pure power based, but also competence based.[2][3] Ultimately leading researchers questioning viability of decentralized organizations as a concept.[4]

This paper introduces a novel protocol designed to address this gap by establishing a dynamic ranking ladder system. Our protocol incentivizes participants to demonstrate their abilities through competitive "elections" within tiered groups. By requiring both time and financial commitment, we create a system that is resistant to Sybil attacks and fosters genuine competence development. This approach can be applied to various decentralized systems, including blockchain consensus mechanisms, where it can contribute to more robust and equitable governance.

This research aims to:

- Propose a methodology for creating a dynamic ranking system in a trustless environment.
- Analyze potential attack vectors and present robust resistance mechanisms.
- Discuss potential applications and benefits of the competence framework.

It is important to note that the proposed protocol is a theoretical construct that relies on having already established consensus mechanism to facilitate the protocol operation. Such could be executed on top of existing blockchain consensus mechanisms.

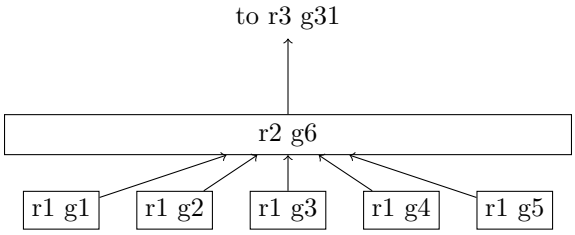

Figure 1: Diagram illustrating the rank ladder. With minimum participant requirements of 5, 30 games are required to create a rank 3 game. Strong candidate would need only 2 wins to reach it.

2 Protocol description

Protocol is based on breaking participants in to smaller groups with singular purpose of electing a winner. This process of election can be implemented as any sub-protocol that can take form of block building challenge, community discussion or more generally data exchange between participants and is not discussed in this paper. The only importance is that it must take multiple participants that must agree on leader, and that leader must be able to be verified by all participants.

In order to make such groups interoperable based on same trust assumptions, yet free to define their own participation parameters, we introduce two distinct principal constant values constituting our protocol: (1) principal time constant P_t and (2) principal asset cost P_c. These serve to create a common price and time relationship between any group to each other. We also add boundary case limitation N_{min} - minimum number of participants required to form a group.

Beside protocol wide constants, we allow Every group to have own properties:

- id - a protocol wide unique group identifier
- N - number of participants
- T - minimum time, agreed by members, that's needed to finalize election
- R - rank
- S - state - can be one of following:
  - **created** - group is created and waiting for participants to join
  - **started** - group is started ts_i time of start is recorded
  - **finalized** - group is finalized

Beyond that, for every participant there are two global properties:

- P_r - rank of participant
- P_g - group id last joined by participant

Participants can change groups only as long as their current and target group are not in "started" state. Whenever a group is started, it is expected to have at least N_{min} participants and it must cause irreversible stake of participation X_i to all participants balance:

$$X_{id} = f(T_{id}) = \frac{P_t \cdot P_c}{T_{id}} \tag{1}$$

these costs further can be broken down in to equal stake subtracted from each participant account whenever group changes it's state to "started":

$$stake = \frac{X_{id}}{N_{id}} \tag{2}$$

the group can be finalized only after T_i has elapsed since group start state transition. Then a winner can be declared and his rank P_r in the state trie incremented to $P_r = P_r + 1$ only if group rank R is equal to P_r before finalization. This process can be repeated and is illustrated on Fig. 1.

The staked assets further distributed in such manner that would avoid creation of positive feedback loop between groups and participants. Example of such would be nullifying these assets, therefore considering that $R+1$ state transition has intrinsic cost of X_{id}.

Dynamic Proof-of-Authority. As one can notice, the transfer of state is unidirectional from assets in to rank, and is time dependant, every transition can be seen as differential equation cost:

$$\$P_r = \$(P_r - 1) + X_{id} \tag{3}$$

while the rate of obtaining any rank P_r itself is a unit step function dependent on time t:

$$P_r(t) = \lfloor \frac{t \cdot P_t \cdot P_c}{T_{min}} \rfloor \tag{4}$$

Frequency domain. Observation in Eq.4 highlights the dynamic nature of the protocol. Since it is showing linear-time invariant property, the dynamic systems theory[5] may be applied to the protocol to analyze its stability and predict its future behavior.

For example, $1/T_{min}$ represents frequency, hence analysis can be applied to understand phase and frequency relationship between groups with all power and system may be analyzed in s-domain used Laplace transforms. Variety of participants using different T_{min} would result a dynamic competence ladder that can produce specific quorums at specific time points.

3 Sybil attack resistance

Ultimate outcome of protocol is representation of competence of an agent by storing his R rank in the state trie. In order to ensure that such representation is not subject to manipulation, we must analyze security concerns.

From a game theoretic perspective, adversary can be a group that produces a winner with R rank that is higher than any other group in the system. However payment requirement defined in Eq. 1 will be proportional to the number of participants in the group, contrary to the stake requirement fair participant is expected to pay (Eq. 2).

While principal components defining fees allows ensure that any winner produced by any group is time and asset effort normalized. For example, in case of $T_{min} = P_t$, then equation 1 reduces to:

$$X_i = P_c \tag{5}$$

If state transition of one participant's rank R requires a commitment from N_{min} participants, such as a participation fee X_i, we can demonstrate that the proposed ranking ladder introduces a non-linear compounding friction for potential malicious actors attempting to manipulate the system.

For such an adversary the particular strategy depends strongly on the particular application of how the agents actually decide on the winner. If such a process is deterministic, the expected cost is simply

$$X_g \cdot N_{min}^R \tag{6}$$

. If an adversary is able to mix in with fair agents who are not sybils, and the process is not fully deterministic, then we can use the mathematical expectation for costs achieving specific rank via sybil attack described as

$$\mathbb{E}[\$R] = X_g \cdot \mathbb{E}[N_{\text{sybils}}(R)] \tag{7}$$

Where $N_{sybils}(R)$ is a number of sybil accounts required to take quorum in a group, and hence obtain rank R.

Actor likeleness and group fragmentation. From Eq. 6 it can be seen that higher groups generally will be more expensive to manipulate, however in practice breaking groups in smaller may be desired to prevent overcomplexity of needed communication. This would imply that due to group fragmentation, an attacker mixing sybil accounts with fair players must strategically allocate accounts across groups for cost efficiency.

Ability for participants to reason about the likelihood of a specific group to be a sybil attack is important in that context. If it seems like a group is likely to be a sybil attack, participants must be able to choose to not join the group. This can be done by reviewing the past state history of participants, groups he is joining and social graph arising from how votes are being allocated and can be done with dynamic systems methodology proposed in the end of previous section.

While providing this level of visibility for participants to reason about may seem challenging, protocols like Continuous Voting Proposing Protocol (CVPP) [6] offer a clear definitions for system that will be transparent and easy to reason about, while in general, an automated system can be used to analyze the state trie and provide a clear view of the system.

Additionally, we can use verification mechanisms, such as proof of location [7] or proof of personhood [8] or from use of quadratic voting systems which already shown to be helpful in blockchain governance field [9][10].

If all results are visible and easy to reason about, then, from outset, this means that for any protocol participant, confidence over group conducting a sybil attack will increase as R of group increase, hence they will be more likely to refuse joining group with such, resulting a sybil attack cost close to Eq. 6:

$$\lim_{R\to\infty} \mathbb{E}[N_{\text{sybils}}(R)] = N_{\min} \tag{8}$$

Where N_{min} is amount of peers required to join the group. Hence, Eq. 6 can be used to estimate cost of sybil attack. At the same time, for the agent who is relying on his pure competence and wins each group fairly, by being able to align agents to vote for him, same cost would be only

$$\$R = stake * R \tag{9}$$

Hence, the agent competence can be put at stake when making a any arbitrary decision that uses R as stake. This may take form of taking privileged action with optimistic approval and so on, only condition required to keep agent game-theoretically fair is that action impact must be lower than the cost of obtaining rank.

$$\$TVL << X_g \cdot N_{min}^R \tag{10}$$

Total value locked must be substantially lower then a cost for obtaining rank due to reason that empirical studies are needed to see how fast will required sybil count converge (Eq. 8) in practice with a different voting systems. This strongly depends on how much stochastic and transparent is such a process.

3.1 Quorum Resonances

As discussed in the previous section, any overt sybil attack requires multiple groups to be held in order to establish a sufficient ranking within the system.

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. Moreover, the Eq. 4 shows that system can be analyzed in time and frequency domains, hence it is possible to analyze sybil attacks not just as a function of time, but also as a function of phase, use complex frequency domain analysis etc.

Also given the initial goal to facilitate protocol for a subjective reasoning matters, it is arguable what it even is - an "sybil attack" or just a "different opinion". Assuming there exist different opinions, and using

the proposed s-domain methodology, competing opinion groups have a way of creating a quorum resonance, where the opinion direction itself can oscillate. All it takes it to have same T_{min} for competing groups that begin their election process at phase difference of π. This can be visualized in following plot 2.:

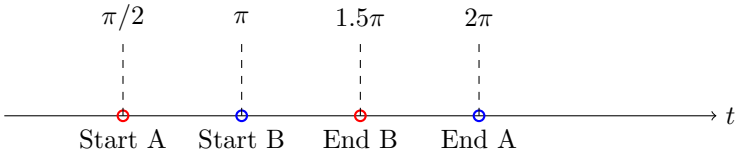

Figure 2: Timing diagram showing two opposite opinion groups finalizing their election process at different time points. The groups have the same T_{min} but with a phase difference of π.

Further, more complicated systems can be imagined, if such groups are many and they allocate their power to reason in alliance manner, creating local quorum resonances, that can be analyzed in frequency domain, and can be used to predict future behavior of the system 3.

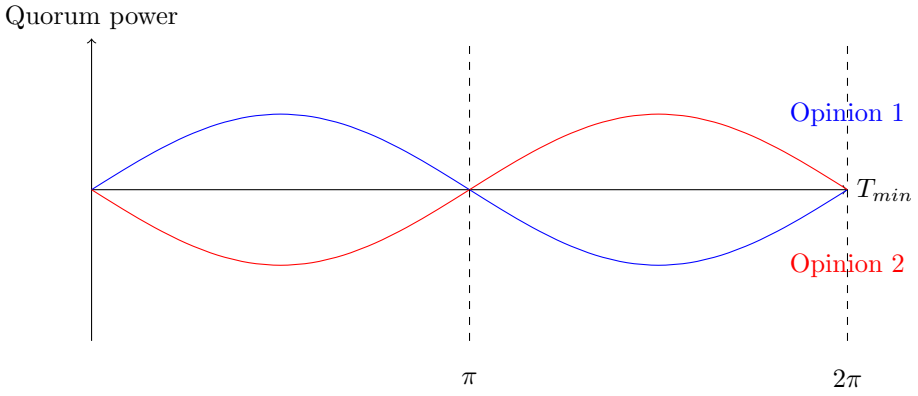

Figure 3: Diagram showing two competing opinion group sets over same subject having their groups T_min same but with same phase difference of π. Sinusoidal waves are for illustrative purpose showing ability of groups to strategically allocate their ranking on time axis, in reality, the groups would have different T_{min} and could be more complex

Utility of the allocated funds

As it can be seen from , the funds allocated cannot be directly used to reward winners and instead must be locked in representation of rank R. If these were to be used to reward winners, the system would be subject to manipulation by the highest bidder. This is a key feature of the protocol that ensures that the ranking system is not subject to manipulation by financial power.

The financial asset however can be used to fund any underlying protocol utility that facilitates the discussion. For example, if used in coupling with CVPP[6], the funds can be used to guarantee data availability of discussion facilitated in the particular group. This would ensure transparency requirements discussed in Sybil attack resistance section. Protocols that allow on-chain payments for long term data availability such as Swarm [11] can be used to ensure that the data is available, by allowing data operators to pull budget from the group's account.

4 Conclusion

This paper introduces a novel protocol for establishing a dynamic ranking ladder system in trustless environments. By leveraging game-theoretic principles and dynamic systems theory, our protocol enables the

autonomous identification of competence while mitigating Sybil attacks. The time-based and cost-based mechanisms ensure that achieving high ranks requires genuine effort and skill and even completely opposite opinions have ability to co-exist.

This protocol offers a promising foundation for building more robust and equitable decentralized governance systems. It has the potential to improve blockchain consensus mechanisms, enhance DAO decision-making, and foster healthier online communities.

Further work is required to analyze the protocol's behavior and effectiveness using dynamic system theory and to explore its integration with existing decentralized platforms.

References

[1] K. Arrow, S. Bowles, and S. N. Durlauf, eds., *Meritocracy and Economic Inequality*. Princeton, NJ: Princeton University Press, 2000.

[2] 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.

[3] R. Fritsch, M. M¨uller, and R. Wattenhofer, "Analyzing voting power in decentralized governance: Who controls daos?," *arXiv preprint arXiv:2204.01176*, no. 2204.01176v1, 2022.

[4] 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.

[5] Lynn and P. A., *The Laplace Transform and the z-transform. Electronic Signals and Systems*. London: Macmillan Education UK, 1986.

[6] T. Pechersky, A. Smirnovs, and A. Soboleva, "Continuous voting proposing protocol for ordering group intents," 2024.

[7] P. Sheng, V. Sevani, R. Rana, H. Tyagi, and P. Viswanath, "Bft-poloc: A byzantine fortified trigonometric proof of location protocol using internet delays," 2024.

[8] WorldCoin, "Private by design." (hhttps://worldcoin.org/privatebydesign-whitepaper).

[9] V. Buterin, Z. Hitzig, and E. G. Weyl, "A flexible design for funding public goods," *Management Science*, vol. 65(11):5171–5187, 2019.

[10] A. Benhaim, B. H. Falk, and G. Tsoukalas, "Balancing power in decentralized governance: Quadratic voting and information aggregation," 2024.

[11] V. TRÓN, "The book of swarm: Storage and communication infrastructure for a self-sovereign digital society." `https://www.ethswarm.org/swarm-whitepaper.pdf`.