Autonomous Competence Identification Protocol: A Dynamic Ranking Ladder System for Blockchain Applications

Tim Pechersky, Aivars Smirnovs

December 15, 2024

Abstract

Meritocratic systems struggle to objectively identify and reward competence. This paper proposes a novel protocol for a dynamic ranking ladder framework in trustless environments. By leveraging game-theoretic principles and dynamic systems theory, our protocol enables autonomous competence identification while mitigating 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, and DAO governance.

1 Introduction

Traditional meritocratic models falter due to the difficulty of identifying and rewarding competence.[1] This challenge is amplified in decentralized systems, where trust is minimized and manipulation is high. Existing consensus mechanisms, such as Proof-of-Work and Proof-of-Stake, only prove participants have computational or financial power, but not necessarily competence to govern the protocol development. This hinders developers from creating robust governance and funding mechanisms that are not purely power-based, but also competence based.[2][3] This leads researchers to question the viability of decentralized organizations.[4]

This paper introduces a novel protocol to establish a dynamic ranking ladder system. Our protocol incentivizes participants to demonstrate their abilities through competitive "elections" within tiered groups. By requiring time and financial commitment, we create a system resistant to Sybil attacks and foster genuine competence development. This approach can be applied to various decentralized systems, including blockchain consensus mechanisms, contributing to more robust and equitable governance.

This research aims to:

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

The proposed protocol is a theoretical construct that relies on established consensus mechanisms to operate. It can be executed on existing blockchain protocols.

2 Protocol description

The protocol breaks participants into smaller groups to elect a winner. This election can be implemented as any sub-protocol like a block building challenge, community discussion, or general data exchange, which isn't discussed here. It involves multiple participants agreeing on a verifiable leader.

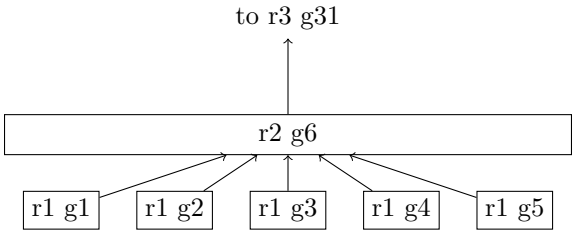

Figure 1: Diagram illustrating the rank ladder. With minimum participant requirements of 5, 30 games are required to create a rank 3 game. Strong candidate would need only 2 wins to reach it.

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

Besides protocol-wide constants, we allow each group to have its own properties:

- id - a protocol-wide unique group identifier
- N - number of participants
- T - minimum time agreed by members to finalize election
- R - rank
- S - state - can be:
  - **created** - group is created and waiting for participants.
  - **started** - group starts ts_i time of start is recorded
  - **finalized** - group is finalized

Additionally, there are two global properties for each participant:

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

Participants can change groups only if their current and target group are not in "started" state. Whenever someone starts a group, it must have at least N_{min} participants and result in an 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 can be broken down into equal stakes subtracted from each participant's account whenever group changes its state to "started":

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

The group can finalize only after T_i has elapsed since the 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 equals P_r before finalization. This process can repeat and is illustrated in Fig. 1.

The staked assets were distributed to avoid a positive feedback loop between groups and participants. For example, nullifying these would incur the intrinsic cost of X_{id}.

Dynamic Proof-of-Authority. The state transfer is unidirectional from assets to rank and time-dependent. This makes every transition a differential equation cost:

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

The rate of obtaining any rank P_r 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. Eq.4 highlights the dynamic nature of the protocol. Since it shows linear-time invariant property, the dynamic systems theory[5] may be applied to analyze its stability and predict its future behavior. $1/T_{min}$ represents frequency, hence phase and frequency relationships between groups exist. Analysis my be done in s-domain using Laplace transforms. Different T_{min} participants would result in a dynamic competence ladder that can produce specific quorums at specific times.

3 Sybil Attack Resistance

The protocol's outcome represents an agent's competence by storing his R rank in the state trie. To ensure this representation isn't manipulatable, we must analyze security concerns.

From a game theory perspective, an adversary can be a group producing a winner with R rank higher than any other group. However, the payment requirement in Eq. 1 will be proportional to the number of participants, contrary to the stake requirement fair participants are expected to pay (Eq. 2).

Principal components defining fees ensure any winner from any group is time and asset effort normalized.

If $T_{min} = P_t$, then equation 1 reduces to:

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

If one participant's rank R transition 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 malicious actors attempting to manipulate the system. The strategy depends on the application of how the agents decide on the winner for such an adversary. If the process is deterministic, the expected cost is

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

If an adversary can mix with fair non-sybil agents and the process is not fully deterministic, 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 the number of sybil accounts required to take quorum in a group and obtain rank R.

Actor likeliness and group fragmentation. From Eq. 6, higher groups are more expensive to manipulate. However, breaking them into smaller ones may prevent communication complexity. This implies that due to group fragmentation, an attacker mixing sybil accounts with fair players must allocate accounts across groups for cost efficiency.

Participants must assess the likelihood of a specific group being a sybil attack. If a group seems likely to be a sybil attack, participants must be able to opt out. This can be done by reviewing the past state history of participants, groups they are joining, and the social graph from vote allocation, using the dynamic systems methodology proposed in the previous section.

While providing this visibility for participants may seem challenging, protocols like Continuous Voting Proposing Protocol (CVPP) [6] offer clear definitions for transparent systems. An automated system can analyze the state trie and provide a clear view.

We can use additional verification mechanisms like proof of location [7] or proof of personhood [8] or quadratic voting systems proven helpful in blockchain governance [9][10].

If all results are visible and easy to reason about, then for any protocol participant, confidence over a sybil attack increases as R of the group increases. This leads to a higher likelihood of refusing to join such a group, 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 the required number of peers to join the group. Eq. 6 estimates the cost of a sybil attack. For an agent relying on competence and winning each group fairly, the cost would be only

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

When making an arbitrary decision using R as stake, this may involve taking privileged action with optimistic approval. The only condition 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 lower than the cost for obtaining rank due to empirical studies needed to see how fast the required sybil count converges (Eq. 8) with different voting systems. This depends on the stochasticity and transparency of the process.

3.1 Quorum Resonances

As discussed earlier, any overt Sybil attack requires multiple groups to establish a sufficient ranking within the system. The intrinsic value of a tokenized competence rating is determined by financial effort, peer success, and time invested in improving one's position. An attacker needs $t_{attack}(R) = t_c \cdot R$ time to reach rank R. This duration allows protocol members to detect and respond to the attack.

The Eq. 4 shows that system can be analyzed in time and frequency domains. This allows Sybil attacks analysis based on time, phase, and complex frequency domain analysis.

Given the initial goal to facilitate protocol for subjective reasoning, it's unclear what a "Sybil attack" or a "different opinion" is. Assuming different opinions exist, and using the proposed s-domain methodology, competing groups can create a quorum resonance, where the opinion direction can oscillate. It takes the same T_{min} for competing groups starting their election process at phase difference of π. This can be visualized in plot 2.:

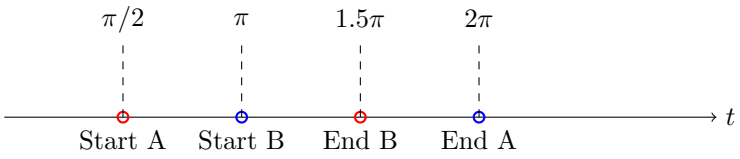

Figure 2: Timing diagram showing two opposite opinion groups completing their election process at different times. The groups have the same T_{min} with a phase difference of π.

If many groups allocate their reasoning power in alliance, more complicated systems can be imagined. These can create local quorum resonances, analyzable in frequency domain, to predict future behavior 3.

Utility of the allocated funds

The allocated funds can't be directly used to reward winners and must be locked in representation of rank R. If 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 the ranking system isn't manipulated by financial power.

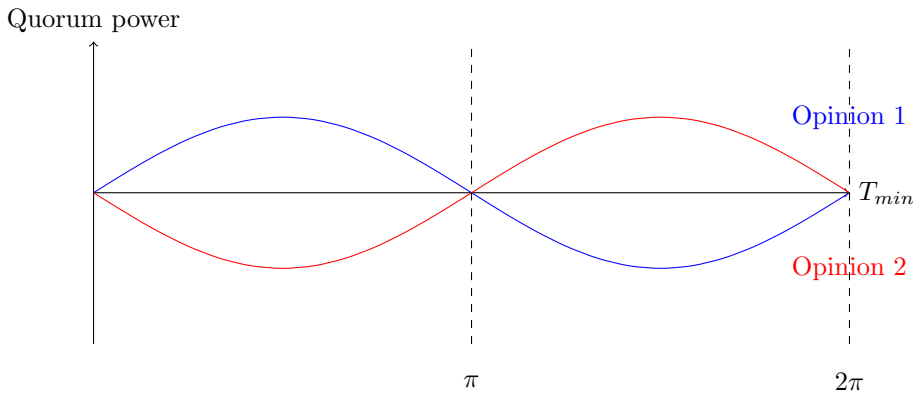

Figure 3: Diagram showing two competing opinion groups over the same subject with the same T_{min} but a π phase difference. Sinusoidal waves illustrate their ability to strategically allocate their ranking on the time axis. In reality, the groups have different T_{min} and could be more complex.

The financial asset can fund any underlying protocol utility for the discussion. If used with CVPP[6], the funds can guarantee data availability of the discussion in a specific group, ensuring transparency in Sybil attack resistance. Protocols allowing on-chain payments for long-term data availability like Swarm [11] ensure data availability by allowing 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. Our protocol enables autonomous identification while mitigating Sybil attacks by leveraging game-theoretic principles and dynamic systems theory. The time-based and cost-based mechanisms ensure high ranks require genuine effort and skill, and opposite opinions can co-exist.

This protocol offers a foundation for building more robust and equitable decentralized governance systems. It improves blockchain consensus mechanisms, enhances DAO decision-making, and fosters healthier online communities.

Further work is needed to analyze the protocol's behavior and effectiveness using dynamic system theory and 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`.