

## Introduction

In the world of decentralized protocols, there's an inherent tension between high-frequency service providers and their low-frequency regulators. At the core lies the challenge: how does a community effectively oversee and regulate service providers that operate at high speeds using a governance mechanism that, by design, takes its time?

## Understanding the Tension

Traditionally, systems aim for harmony between service speed and oversight. However, in the decentralized space, there's a deliberate decision to maintain a slower pace for governance. This ensures decisions are thoroughly vetted, deliberated upon, and agreed upon in consensus. Yet, the very agents it governs — service providers to the protocol — need to provide their services at much higher speeds for the network to fulfill its value.

## Arthur-Merlin Protocols: A Primer

Before diving deeper, it's instructive to turn to complexity theory. Here, Arthur-Merlin protocols provide an interesting insight. In these protocols:

- Arthur

, the verifier, is a probabilistic polynomial-time entity.

- Merlin

, the prover, has unbounded computational power.

Merlin seeks to convince Arthur of certain truths, even though Arthur might be skeptical due to Merlin's superior computational abilities. Traditionally, Arthur is visualized as a single entity.

## From Arthur-Merlin to Decentralized Communities and Permissionless Service Provisioning

Our situation with decentralized protocols mirrors the Arthur-Merlin dynamic but adds two forms of complexity:

### 1. Arthur's Decentralization:

Instead of a singular entity, Arthur becomes a decentralized community. It's within this community that we find solace in the "honest majority" assumptions, given its collective, consensus-driven nature.

### 1. Powers Beyond Computation:

Merlin isn't just a powerhouse of computation. In our scenario, Merlin(s) provides package routing, matching, and other services and assurances about their performance to the network.

## Directions for Proposed Governance Mechanism: Demonstration-Reward Protocol

To bridge this divide between the "slow" decentralized community and the "fast" service provider, we propose that the protocol:

### 1. Reward Demonstrations:

Encourage the community to showcase profitable attacks that go unnoticed when carried out by the fast-paced service providers. This brings vulnerabilities to light.

### 1. Reward Detections:

Compensate for the detection attacks. This makes it economically viable for fast actors to safeguard the system.

Both rewards should be inversely proportional to the number of teams who achieve a given demonstration or detection. This is both needed for anti-sybil mechanics, (through it does create an economic incentive for collusion between different red-teams) and to estimate the value of the attack.

## Navigating the Challenges

### 1. Authenticity Assessment:

How do we gauge the genuineness of an attack or demonstration?

### 1. Economic Balancing:

Ensuring that rewards are substantial enough to encourage auditing, but that the costs this imposes on the network do not limit its appeal.

Directions for ongoing work

The intricate dance between high-frequency services and low-frequency governance in decentralized protocols will require careful planning and robust mechanisms. Drawing parallels with established theories, like the Arthur-Merlin protocols, offers a initial lens through which we can begin to approach these challenges. As we continue refining this approach, the ultimate goal remains: a resilient, secure decentralized network.