Validator Challenge #8 — “Great Experiments”

Security note (READ FIRST):
Do not reuse Mainnet keys. This includes both wallet keys and validator keys.
Use your dedicated BoN wallet and BoN validator keys only.

Goal

Design and run your own experiments on the BoN testnet. The goal is to generate useful signal ahead of mainnet launch — whether by validating that network and node operations work correctly, monitoring node behavior under specific conditions, or pushing the network to its limits with adversarial or edge-case setups.

This challenge rewards curiosity and rigour. There are no prescribed test cases. Validators are encouraged to explore any angle they think is relevant — and are explicitly encouraged to surface potential vulnerabilities, which feed into the Protocol Security Track.

What to Submit

You may submit up to 3 experiments. Each submission must include:

1. **Title —** a short, descriptive name for the experiment
2. **Setup description —** brief description of the configuration or environment used
3. **Actions description —** brief description of what was done and how
4. **Notes** (optional) — any additional context, observations, or caveats
5. **Evidence —** logs, results, or proof, submitted as a shareable folder link (Google Drive, Dropbox, or equivalent public cloud storage)

Submissions are made via the competition portal at bon.multiversx.com. Deadline: Monday, March 30th, 12:00 UTC.

Scope

Experiments may cover any of the following (non-exhaustive):

- Validating correct behavior of network or node operations under specific configurations
- Monitoring node behavior over time or under load
- Adversarial testing: deliberate misbehavior, edge-case inputs, resource exhaustion, timing attacks

- Protocol correctness checks: verifying state transitions, consensus edge cases, epoch boundary handling
- Infrastructure resilience: failover, hot-swap, geographic latency, connectivity degradation

Out of scope - Volumetric DDoS attacks with no protocol-level insight are not considered admissible experiments (they do not reveal useful network behavior and may degrade the environment for other participants).
- Attacks on shared infrastructure (public gateways, explorers, APIs, the BoN portal) — focus on your own node and protocol behavior.
- Attacks on other participants' nodes or machines.
- Social engineering, phishing, or credential theft attempts.
- Experiments on mainnet or non-BoN testnets.
- Re-running known, publicly documented issues without a new hypothesis or angle.

Scoring

Base points

500 points are awarded for each admissible experiment, up to a maximum of 3 experiments (1,500 points total).

An experiment is admissible if it includes all required fields, the evidence link is accessible, and the setup is non-trivial and relevant to network operation.

Discretionary bonus points

The MultiversX engineering team will review all submissions and may award bonus points per experiment on the following scale:

Condition	Bonus Points
+50 — Sound methodology: clear hypothesis, well-chosen test case, results clearly documented. The experiment tests something non-trivial and is easy for reviewers to follow and reproduce.	**+50**
+75 — Creative or novel design: tests something non-obvious or underexplored; the setup itself is inventive and adds value regardless of the outcome. A clean pass here is as valuable as a finding.	**+75**
+100 — Exceptional: highly rigorous, tests something the team had not previously considered, produces clear and well-documented results. Whether the outcome is a confirmed vulnerability or a validated clean behavior, the experiment is independently valuable to the network.	**+100**

> Bonus points are awarded at the engineering team's discretion. A single experiment can receive at most one bonus tier. Bonus awards will be published alongside final results.

Maximum score for Challenge #8: **1,800 pts** (3 experiments × 500 base + 3 × 100 bonus)

→ **EXAMPLE SUBMISSION**

Connection to the Security Track

This challenge is intentionally designed as an exploratory phase that feeds into the Security/Protocol Integrity Track. If your experimentation surfaces anything that looks like a vulnerability or unexpected protocol behavior, submit it to the Security Track as well — it will be evaluated independently for the separate $50K EGLD prize pool.

Submitting to the Security Track does not affect your score here. The two tracks are fully independent — a finding can qualify for both.

FAQ

Q: Do I need to show a positive result? What if my experiment is inconclusive?

A: No. Inconclusive results are admissible provided the setup and methodology are sound. A well-documented null result (i.e., the network behaved as expected) still provides useful signal. The bonus tiers reward insight and findings, not just activity.

Q: Can I submit multiple experiments covering the same area?

A: Yes, but each submission should represent a distinct setup or hypothesis. Submitting three near-identical experiments with minor variations will not be treated as three separate entries.

Q: What format should the evidence folder follow?

A: No strict format is required. Include whatever logs, outputs, screenshots, or notes allow the reviewers to understand and reproduce your experiment. Clearly label files so reviewers can navigate them without guesswork.

Q: If I find a vulnerability, should I disclose it publicly first?

A: No. Report it through the Security Track via the official submission channel. Do not post vulnerability details publicly before the engineering team has reviewed and acknowledged the report.