Summary of Indigo Protocol V2 Audit

The auditing of smart contracts, especially in the burgeoning field of decentralized finance (DeFi), plays a pivotal role in ensuring the security, efficiency, and reliability of blockchain protocols. This summary delineates the audit process, timeline, methodology, and findings for the Indigo Protocol V2, conducted by the MLabs Audit Team.

Importance of Auditing Smart Contracts

Smart contracts are immutable once deployed on the blockchain, making pre-deployment audits crucial to identify vulnerabilities, ensure compliance with specifications, and safeguard against potential exploits by malicious actors. This audit process is indispensable for maintaining user trust, securing investments, and facilitating a robust DeFi ecosystem.

The Process of the Indigo Protocol V2 Audit

Audit Scope & Parties Involved
The audit, conducted by the MLabs Audit Team, encompassed an examination of the smart contract code with the aim of identifying security vulnerabilities, deviations from specified requirements, and areas for optimization in code quality. The MLabs Audit Team is distinct and separate from the development team, to avoid conflicts of interest and help ensure an unbiased and comprehensive analysis of the smart contract's security posture.

Methodology
The audit process was divided into distinct phases to ensure thorough coverage of the protocol’s code and associated documentation. The timeline was structured as follows:

- **Initial Exploratory Phase:** The audit began with a detailed review of all modules to understand the protocol’s architecture, functionalities, and codebase. This stage aimed to acquaint the auditors with the protocol's details and prepare for deeper analysis.
- **Structured Exploration Phase:** This phase involved detailed investigations into each smart contract's potential vulnerabilities, supported by penetration testing over four sprints. A round-robin approach ensured exhaustive scrutiny of each component, facilitating comprehensive codebase coverage and finding verification.
- **Reporting Phase:** Marking the end of the primary audit phase, this sprint focused on compiling the audit findings into a report, categorizing vulnerabilities by severity and noting any incorrect specifications and code quality concerns.
- **Reviewing Proposed Fixes:** The final sprints concentrated on evaluating all proposed fixes and investigating additional vulnerabilities, especially concerning the upgrade minting policies and the V2 deployment checklist. Each fix was individually assessed to confirm its effectiveness.

The initial audit report was handed over to the Indigo Labs team on March 14th, 2024. The Indigo Labs team responded to the initial audit report on March 22nd, 2024. The MLabs team responded with its final audit remediation report on March 29th, 2024.

Summary of Findings

The initial audit identified a few vulnerabilities ranging in severity from high to low, potential optimizations, as well as issues in code quality that could impact the readability and maintainability of the codebase. Each item from the audit report was reviewed by the Indigo Labs team and addressed.

Conclusion

The MLabs Audit Team has provided detailed findings and recommendations to enhance the security and reliability of the Indigo Protocol V2. The Indigo Labs team is thankful in their cooperation and diligent efforts in providing a complete, detailed audit report.