Smart Contract Hacker and Developer Internship Report

Anmol Dhiman

Cooperative Kleros

January 29th, 2024 - July 29th, 2024

Mentor - JB

Table of Contents

Executive Summary

This internship report provides an overview of my time at Kleros, where I engaged in smart contract reviews, dependency updates, issue resolutions, and development tasks. I worked on key components of Kleros infrastructure, including v1 and v2 contracts, conducting thorough reviews and developing new features.

Key projects included reviewing the KlerosLiquid.sol contract, zk cross chain realitio proxy contracts, and quick review for vulnerabilities in KlerosCore, DisputeKitClassic, SortitionModule, and DisputeResolver contracts. I assisted with the migration to OpenZeppelin v5, updated Solidity versions for over 116 Kleros v2 and VEA contracts, and improved the development environment by updating dependencies like Hardhat, Hardhat-deploy, and Ethers.js. I also developed deterministic deployment scripts for deterministic addresses on different chains.

In addition, I reviewed the Proof of Humanity (PoH) v2 contract and built a Redstone proxy contract.

My internship at Kleros was not only about technical growth but also about developing essential soft skills. Effective communication was crucial for conveying technical details and collaborating with team members. Teamwork played a significant role in fostering a productive work environment, while problem-solving skills were honed through tackling complex technical challenges. Time management was vital in balancing multiple projects and meeting deadlines, and adaptability was demonstrated by embracing new tools, technologies, and workflows.

Introduction

Kleros is a decentralized dispute resolution platform that utilizes blockchain technology to provide fast, secure, and affordable arbitration services. Founded on the principles of transparency and decentralization, Kleros aims to democratize the arbitration process by leveraging the power of smart contracts and a distributed jury system.

Kleros' mission to provide transparent and fair dispute resolution using cutting-edge blockchain technology aligns perfectly with my passion for leveraging technology to solve real-world problems.

Kleros operates on a unique model that integrates smart contracts, crowdsourced jurors, and Schelling Point to resolve disputes. This innovative approach reduces costs and ensures that the arbitration process is swift, impartial, and affordable. This model democratizes processes that have traditionally been opaque, inaccessible, expensive, and time-consuming to many.

My primary objective during the internship was to gain hands-on experience in smart contract development and security auditing. I worked on several critical projects that were integral to the enhancement of Kleros' core infrastructure. This included reviewing and updating smart contracts to ensure they were robust and secure.

One of the most rewarding aspects of my internship was the ability to contribute directly to the improvement of the Kleros platform. Whether it was through conducting detailed contract reviews, updating dependencies, or developing new features, each task provided a learning opportunity and a chance to make a tangible impact.

Description of Duties and Accomplishments

During my internship, my main responsibilities included conducting security reviews of smart contracts, refactoring and maintaining the smart contract codebase to keep it up to date with dependencies, developing new smart contracts, writing comprehensive test cases using Hardhat, and creating deployment scripts to streamline the deployment process. Below are the key projects and accomplishments :

1. Review of KlerosLiquid.sol Contract -
    - I carried out a thorough review of the KlerosLiquid.sol contract, which is the v1 of the Kleros Dispute Resolution system. My review focused on finding any potential vulnerabilities and making sure the contract followed best practices. I carefully examined the code to ensure it was secure and reliable, and then I put together a detailed report outlining my findings and suggestions for improvements.

2. Review of zkSync Cross Chain Realitio Proxy-
    - Reviewed the zkRealitioHomeProxy and zkRealitioForeignProxy contracts, which consist of two components: the Home proxy on the zkSync chain and the Foreign proxy on the mainnet. These contracts facilitate arbitration services on the zkSync chain. My primary focus during the review was on the functionality and the implementation of the bridging mechanism.
    - Shared a detailed report outlining my findings and suggestions for improvements.

3. Quick Review of Money Stealing for KlerosCore, DisputeKitClassic, SortitionModule, and DisputeResolver Contracts -
    - I conducted a quick review of these contracts to identify any potential vulnerabilities that could lead to theft, as they were scheduled for deployment on the Arbitrum mainnet. Fortunately, no critical vulnerabilities were found.

4. #1270 Openzeppelin v5 migration in Kleros v2 and VEA -
    - The OZ v5 migration involved adding namespace storage formats to proxy contracts.
    - In Kleros v2, I updated the proxy contracts with the required changes (PR), while in VEA, it was mainly a dependency version update (commit hash).
    - These updates were successfully implemented, ensuring compatibility with the existing codebase.

5. #1510 & #280 Solidity Version Update in Kleros v2 and VEA -
    - Updated the Solidity version for Kleros v2 and VEA contracts, modifying them to be compatible with the latest Solidity features and improvements.
    - Updated over 116 contract files to reflect the new Solidity version.
    - Successfully released the vea-contracts npm package to ensure compatibility with Kleros v2 contracts.
    - Proof-of-work: Kleros v2 PR and VEA PR

6. #100 Deterministic Deployment Scripts in Kleros v2 -
    - Developed deterministic deployment scripts for Kleros v2 contracts, ensuring that the contracts are deployed to the same address across all chains, thereby improving the reliability of the deployment process.
    - Made changes to base, core, and neo of Kleros v2 contracts to implement this feature, ensuring compatibility with existing test cases.
    - Refactored the test cases to address failures caused by the consistent address deployment.
    - Proof-of-Work: PR

7. #1606 Hardhat, Hardhat-Deploy, and Ethers Update in Kleros v2 -
    - This task involved updating the dependencies to the versions used in Curate v2 and Escrow v2, ensuring the projects utilize the latest and most secure libraries and tools.
    - These updates resulted in minor changes across nearly all test files and deployment scripts. I refactored the affected files and scripts to accommodate these changes, ensuring the continued functionality and integrity of the system.
    - Proof-of-Work : PR

8. Review of Proof of Humanity v2 -
    - Conducted a comprehensive security check for PoH v2 to ensure that the functionality was implemented correctly.
    - Reviewed the documentation thoroughly to understand the project's functionality, then shared my findings and suggestions in a detailed review report.

9. Review of Arbitrum Cross Chain Realitio Proxy -
    - Reviewed the RealitioForeignProxyArb and RealitioHomeProxyArb contracts, which consist of two components: the Home proxy on the Arbitrum chain and the Foreign proxy on the mainnet. These contracts facilitate arbitration services on the Arbitrum chain.
    - Ensure that both the functionality and bridging system were correctly implemented.
    - Reviewed the Arbitrum bridging mechanism documentation to understand the project's functionality and shared my findings and suggestions in a detailed report.

10. Developed Redstone Cross Chain Realitio Proxy Contracts -
    - Explored how the bridging system works in the Redstone Chain, noting how it differs from systems used in Arbitrum and zkSync.
    - Developed proxy contracts and mock versions for testing, ensuring they functioned correctly and reliably.
    - Created deployment scripts to set up the main protocol address on Redstone and Ethereum mainnet. Also, refactored scripts for testing on Optimism's Sepolia and Sepolia chain testnets to ensure everything works smoothly in different testing environments.
    - Collaborated with Danil and Manmeet to get an initial review of the protocol and integrated their suggestions for improvement. - Danil's Report and Manmeet's Report.
    - Received the mitigation review report from Danil, made necessary adjustments based on it, and now the protocols are prepared for testing. - Danil's Report

Skills Learned

During my internship at Kleros, I developed several new skills and enhanced existing ones :

❖ **Technical Skills** :

1. Development Automation -
   - Learned about development automation, including conventional commits, GitHub actions, and Slither automated testing.
   - Learned how to use the Yarn workflow, essential for organizing and constructing project components.
2. Smart Contract Auditing and Development -
   - Enhanced auditing skills by adopting a hacker mindset, focusing on finding vulnerabilities to exploit.
   - Worked on large, complex projects, sharpening the ability to identify and address security issues effectively.
   - Developed a keen eye for detail and a strong understanding of security best practices in smart contract development.
3. Security Tools and Best Practices -
   - Enhanced skills using security tools such as Slither, Aderyn, Foundry (for fuzz testing), Echidna, and Manticore.
   - Learned extensively about best practices in development and security review from the Smart Contract Security Field Guide.
   - Accessed numerous resources that contributed to my growth as both a security researcher and a smart contract developer.
4. Blockchain Concepts -
   - Learned key blockchain concepts such as Chainlink VRF, Optimism Bridging mechanisms, Upgradability, and Shelling Points.
   - Broadened understanding of the technical and theoretical aspects of blockchain technology.

❖ **Soft Skills** :

1. Communication -
    - Significantly improved communication skills.
    - Learned to express ideas clearly and concisely, ensuring team members understood project goals and updates.
    - Effective communication kept the team on the same page and encouraged a supportive atmosphere.
2. Adaptability -
    - Quickly adjusted to different projects and timelines, embracing changes with enthusiasm.
    - Learning new skills and approaches was exciting, highlighting the importance of flexibility in a fast-paced environment.
    - Adaptability contributed to personal growth and the dynamic and innovative spirit at Kleros.
3. Problem Solving -
    - Improved problem-solving skills by addressing development issues where updates sometimes break existing systems.
    - Learned to methodically diagnose issues, find root causes, and apply effective fixes, validating solutions through proper testing.
    - Experience in handling complex challenges ensured smooth project execution and enhanced problem-solving abilities.

I've developed valuable technical skills in automating development processes, auditing and developing smart contracts and understanding blockchain concepts. These experiences have deepened my knowledge of blockchain technology and equipped me with practical expertise in security tools. On a personal level, I've improved my ability to communicate, adapt to new challenges quickly, and solve problems effectively. These skills will undoubtedly benefit my future career aspirations, particularly in my goal of becoming a security researcher and developer.

Conclusion

My internship at Kleros was a highly rewarding experience, offering valuable insights into smart contract development and security. Working on critical projects allowed me to contribute directly to enhancing Kleros' infrastructure, honing my technical skills, and deepening my understanding of blockchain technology.

In addition to technical growth, the internship also refined my soft skills, including communication, teamwork, and problem-solving. These experiences have been instrumental in my professional development and will greatly benefit my future endeavors in the blockchain industry.

Being part of a talented and supportive team at Kleros was incredibly beneficial. It taught me the importance of business culture in fostering rapid development and provided insights into how blockchain businesses operate. Having previously worked in small, team-based startups, this experience broadened my perspective on larger-scale operations. I’m particularly excited by real-world problem-solving and find the potential applications of dispute resolution and Proof of Humanity (PoH) fascinating. These technologies offer solutions to significant challenges and represent important advancements in the decentralized and DeFi spaces.