AUDITING A NOVEL DISTRIBUTED LEDGER

Summary

The client approached FP Complete for code review and audit services. Our prior work in the related space of blockchain project audits provided us the theoretical background necessary to understand the overall architecture, project requirements, and goals.

Our goal was to review the existing codebase, compare against the whitepaper specifying the design, and provide concrete, actionable items to help the team improve the code from a maintenance, performance, and security standpoint.

Industry: Distributed ledger/cryptocurrency
Project Type: Audit/code review
Technology Used: Java

Project Requirements

The project in question was separated into multiple layers of functionality. FP Complete was tasked initially with reviewing the code for the highest, client-facing layer of functionality, and to provide feedback. The scope was relatively open-ended. The goal was to identify potential improvements across the board.

Over time, the scope evolved to include further components of the project, including the lower layer of functionality, testing practices, and whitepaper analysis. Ultimately, we were asked to provide a complete report on the project's evolution over our multi-year engagement for public consumption.

The Solution

FP Complete's team applied an iterative audit approach. Each stage of review work focused on a single commit in the project's history. We iterated regularly with the engineering team at the client to receive feedback. We were particularly impressed by the responsiveness of the client to our requests for information and recommendations for improvement. Many issues were resolved before we could complete the audit phase itself.

After each phase was complete, the client team would work further on integrating our recommendations, as well as implement further feature work. Our iterative process then kicked in. When a new version of the code was available, we would analyze the difference between the two code commits for our further analysis.

Throughout, we leveraged code analysis tools to uncover common areas for improvement. We analyzed dependencies for known vulnerabilities. We inspected test coverage reports. And finally, we inspected the code manually to provide feedback, especially focusing on potential security concerns.

New Challenges for FP Complete

This was the first project we engaged with that involved a proof assistant language, Coq, leveraged in ensuring correctness. Fortunately, some of our non-audit team had prior experience with this language. This introduced a new code review methodology into our workflow.

Additionally, the fast-paced iteration process with the client's engineering team was unexpected. Typically, our reports chronicle multiple person-months of review, followed by an implementation phase. Working more directly with the client's team allowed for a different, and in our opinion more productive, workflow.

Conclusion

Through our efforts on this project, we were able to assist a smart, competent, experienced engineering team further improve their code quality. Complex distributed systems are always difficult to design and implement correctly. We take pride in being able to assist such a complex piece of software come to market with confidence.