Scroll

Navigating zkEVM Challenges

How Trail of Bits enhanced Scroll's security framework

Scroll, a company aimed at extending Ethereum's capabilities through zero-knowledge (ZK) technology and EVM compatibility, faced the challenge of auditing its zkEVM circuits.

The initial challenge was the scarcity of teams with the requisite expertise in ZK circuit security testing and with Halo2 specifically. Scroll engaged with multiple firms, assessing their understanding and capabilities in this niche area.

The choice to engage Trail of Bits was ultimately driven by strong references, previous positive experiences, confidence in their expertise, and practical considerations such as timing, availability, and cost.

45.8	Engineer weeks w/ 6 consultants	**17**	High-severity issues
5	Custom Semgrep rules for targeting Halo2	**7**	Medium-severity issues
40	Informational issues	**6**	Low-severity issues

> "Trail of Bits' insightful ZK research further showcased their technical capabilities, serving as a solid reference for their expertise"

Haichen Shen,
Co-founder, Scroll
on working with Trail of Bits

Public Assessments

Scroll ZkEVM Wave 1
April 17 to June 23, 2023 | **23 engineer-weeks**
Circuit soundness and the correct implementation of the EVM semantics

Scroll ZkEVM Wave 2
July 17 to August 4, 2023 | **6 engineer-weeks**
Ensuring the circuits are sound, complete, and faithful implementations of the specifications

Scroll ZkEVM Wave 3
August 14 to September 19, 2023 | **9 engineer-weeks**
Soundness and completeness of circuits

Scroll zkTrie
June 26 to July 11, 2023 | **4 engineer-weeks**
Checking for inclusion and non-inclusion proof verification, data structure correctness, and safe and reliable bindings

Effective use of tooling

Trail of Bits provided Scroll with instructions on every auditing tool used to uncover issues during the engagement.

> **Static Analysis: Semgrep, CodeQL**
> **Rust: Clippy** `cargo-audit cargo-edit cargo-llvm-cov`
> **Go:** `golangci-lint Go cover`

Trail of Bits also provided custom Semgrep rules built specifically for Scroll. This allowed Scroll to incorporate these tools into its CI/CD pipeline to ensure common mistakes, non-idiomatic code, and repeat vulnerabilities are not introduced into the codebase. In particular, Trail of Bits developed a custom analysis of Halo2 circuits with Semgrep to identify specific security vulnerabilities during the assessment. This analysis ensures that no variants of these vulnerabilities exist in the codebase and, if incorporated into CI/CD pipeline, prevents the reintroduction of these vulnerabilities in the future.

Long-term security improvements

The assessment conducted by Trail of Bits proved to be highly effective, showcasing their thorough understanding of ZK circuits and a proactive approach that underscores their expertise. Trail of Bits' insightful and actionable findings offered Scroll invaluable lessons in coding practices and ZK circuit development. These recommendations were instrumental in enhancing Scroll's security posture and refining its development and design processes. Trail of Bits' comprehensive approach led to the development of cleaner code and significantly reduced the likelihood of errors, strengthening Scroll's approach to preempting potential issues in future developments.

> "Trail of Bit's recommendations of certain tools and scripts for sanity checks during development have been beneficial for long-term improvements"
>
> Haichen Shen, Co-founder, Scroll
> on working with Trail of Bits

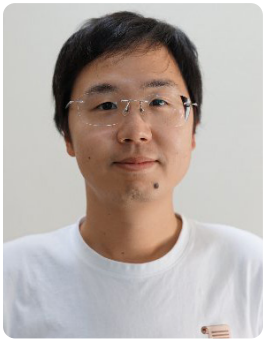
Effective communication

The communication between Scroll and Trail of Bits was characterized by its high quality, highlighted by the weekly progress reports and calls, a practice not universally adopted by all auditing firms. These regular interactions facilitated prompt responses to assessment findings and served as a platform for productive discussions. This level of engagement significantly enhanced Scroll's understanding of the review process and enabled a more thorough examination of their codebase, contributing to the overall effectiveness of the assessment and the improvement of their development practices.

Scroll welcomes more public reviews on their zkevm circuit implementation.
If you find any vulnerabilities in their circuit, please email Scroll at **security@scroll.io**

Background on Haichen Shen

CO-FOUNDER, SCROLL



Haichen Shen, co-founder at Scroll, has a notable background in open-source projects like zkEVM and Apache TVM. With a Ph.D. in computer science from the University of Washington and prior experience as a senior applied scientist at Amazon Web Services, Haichen has contributed significantly to cryptography and blockchain technology.

He has authored and co-authored many publications, including Nimble: Efficiently Compiling Dynamic Neural Networks for Model Inference and Nexus: a GPU cluster engine for accelerating DNN-based video analysis.

Resources to learn more:

KNOWLEDGE:

- ZKDocs
- Serving up zero-knowledge proofs

TOOLS:

- It Pays to be Circomspect
- Amarna: Static analysis for Cairo programs

SPECIFIC VULNERABILITIES:

- Weak Fiat-Shamir Attacks on Modern Proof Systems
- Specialized Zero-Knowledge Proof failures
- A mistake in the bulletproofs paper could have led to the theft of millions of dollars
- Disclosing Shamir's Secret Sharing vulnerabilities and announcing ZKDocs