ZPrize Winners Craft 1,028% Faster Proof Speeds

Alternative headlines:
One Giant Leap for ZK: How Trapdoor Tech Got 1,028% Proof Speeds
Aleo-Funded ZPrize Competition Leads to 1,028% ZK Proof Speeds

By Nick Fouriezos

Zero-knowledge proofs have justifiably received significant attention from developers for their promise in enabling a more secure, private, and scalable web.

However, to realize their full potential for mass adoption, ZK applications will need to be fast enough to verify proofs at the type of speeds that traditional internet users have grown accustomed to.

ZPrize co-sponsor Aleo, a privacy-preserving blockchain with built-in ZK capabilities, is committed to accelerating innovation throughout the entire ZK cryptography space — which is why Aleo offered 2M Aleo Credits to the team that could develop the fastest verifier using Marlin, a universal and updateable ZK proof system that undergirds Aleo and other ZK enterprises.

The results of the competition were a significant step for the entire ZK ecosystem. Each finalist exponentially improved upon current Marlin verification speeds, creating open source solutions that anybody can use to advance privacy on the web.

Paradigm-shifting results

On a public blockchain network, validators must construct blocks out from submitted user transactions in batches over a prescribed interval. Doing this as efficiently as possible is important for scalability in any zk-based L1 or L2.

In this competition, teams were asked to create systems that would optimize to …

- Verify as many batches of Marlin proofs as possible in a 10-second period.
- Minimize total cost while doing so.

Teams were judged on both the accuracy and speed of their proofs. Their results marked a monumental shift in past performance standards.

POSITION	TEAM NAME	SCORE	% IMPROVEMENT	REPOSITORY
1	先河ARS	11.29	1028.60%	→ View Here
2	Supranational	5.92	492.00%	→ View Here
3	ANONYMOUS	2.33	133.33%	→ View Here
4	ZPrize (Baseline)	1	0.00%	→ View Here

(To view the full results and repository, click here)

What worked, and why

Trapdoor Tech, Supranational and Anonymous all were able to realize significant computational improvements over the ZPrize baseline performance of **XX.**

1st Place: Trapdoor Tech (+1,028.60% Improvement)

Trapdoor Tech specializes in developing real-world applications with zk-SNARK/STARK technology — particularly excelling in their adept use of Graphic-Processing Units and Field Programmable Gate Arrays to improve ZK performance. The team does a great job breaking down the various technical logics and models underpinning ZK technology here.

In essence, Trapdoor Tech is able to achieve significant performance improvements by understanding the benefits of both GPUs and FPGAs, and using those advantages and disadvantages strategically.

As of now, GPUs have a significant price advantage, shorter development times and substantial parallelism from the get-go — plus an abundance of GPUs that currently are being under-utilized because of the Ethereum switch to Proof of Stake, making it a buyer's market for those in need of GPU services.

However, FPGAs have long-term advantages in power consumption, and already provide better latency in high-speed data streams, with FPGA clusters outperforming GPU clusters, as this article by hardware provider Ingonyama outlines.

While completing the challenge, Trapdoor Tech was also able to innovate a process that required fewer calculation rounds to verify proofs, which could be pivotal to improving processing speeds and furthering zk integration into future applications.

“The bottleneck right now for integrating zero-knowledge onto blockchains is proof generation. If you improve that performance, you improve transaction-per-second rates a lot,” Trapdoor Tech founder Star Li told ZPrize.

2nd Place: Supranational (+492% improvement)

Supranational, the runner-up in this category, has substantial expertise in hardware acceleration of cryptography and open-source cryptography. The founding team worked at Intel and was involved in projects like the Intel SHA extensions, while other team members have been long-time contributors to open source cryptography libraries that power the modern web, like OpenSSL.

Supranational created the blst library, which powers cryptography for protocols like Ethereum, Filecoin, Aptos, Sui, Flow, and more. The team also developed sppark, a library used as the baseline in the MSM track of ZPrize 2022 competition and currently incorporated into live zero-knowledge protocols like Aleo.

“The FPGA track was particularly interesting as it involved hardware design, one of the core competencies of the Supranational team. The FPGA competition was also challenging as it required a number of skill sets such as algorithm design, hardware implementation, and memory optimization,” Supranational Co-Founder Kelly Olson told ZPrize.

How to participate in the next ZK wave

The promise of zero-knowledge was once purely academic. No longer.

ZKPs and their potential to enable greater privacy and scalability on the web has, justifiably, gotten more attention as real-world use cases increasingly emerge. Intellectual exercises are moving closer to becoming digital realities, at the exact same time that web users are demanding more control over their data, and who has access to it, than ever before.

However, there are still significant hardware hurdles for ZK to reach its full potential in giving people more control over their digital footprints.

To help move the entire web3 space closer to that reality, Aleo’s Alex Pruden and a collection of top technologists and cryptographers from across the web3 sphere — including representatives of full list here — have invested millions of dollars in grants to fund the next wave of ZK technology for the world.

Want to build the future of ZK? The categories and deadlines for ZPrize 2023 are up, and still accepting submissions.

Head to our Discord to find out more.