NEWS RELEASE

Fermah Closes $5.2M Seed Round to Abstract Away the Complexity of ZK Proof Generation

2024-09-17

NEW YORK, Sept. 17, 2024 /PRNewswire/ -- **Fermah**, the universal proof generation layer, has announced the successful closure of its $5.2 million seed round, co-led by the a16z CSX fund and Lemniscap. The round also included participation from Bankless Ventures, Longhash Ventures, P-OPS team, Public Works, ZK Validator, Lambda Class, Daedalus, Zero DAO, Velocity Capital, and Daemon Ventures.

A number of S-tier builders also participated as angels in the round, including former Coinbase CTO and a16z GP Balaji Srinivasan; Celestia's Mustafa Al-Bassam (CEO) and Nick White (COO); Co-founders of Polygon, Sandeep Nailwal, Jaynti Kanani, and Daniel Lubarov; as well as Aztec's Zac Williamson (CEO) and Claire Kart (CMO); and several others.

The funding will go towards product development and team expansion, with Fermah currently **hiring** for a number of key roles, as part of the company's vision to make zero-knowledge proofs the default substrate for all computation.

Fermah was founded by seasoned cryptographer Vanishree Rao, who has dedicated the last 15 years to designing and building Zero-Knowledge Proofs (ZKPs), and holds a PhD in Cryptography from UCLA. Vanishree was also the Lead Cryptographer at O(1) Labs – the team behind Mina Protocol, one of the earliest and most innovative ZK protocols. She has extensive experience working with cryptographic primitives including secure hash functions, advanced digital signature schemes, ZKPs, multi-party computation protocols, key exchange protocols, and program obfuscation.

While ZKP technology is slowly becoming practical enough to power broad, modern applications, the generation of proofs remains extremely resource-intensive, requiring expensive, powerful physical infrastructure. The underutilization of this hardware inflates the price users pay for their ZK transactions. Beyond this, designing, implementing, and maintaining the optimal incentive structure for this infrastructure is extremely onerous.

Fermah – which is optimized for cheap, fast, and reliable ZK proof generation – is addressing this long-standing complexity issue inherent to ZKPs, functioning as a marketplace for ZK proof generation. Fermah generates proofs for any instance in which ZK is used – whether it's for ZK rollups, ZK bridges, ZK coprocessors, ZKML projects or ZKFHE projects. Fermah is neutral and architected to support all proof systems, including zkVMs, zkEVMs, Groth16, and all other proof systems.

Fermah aggregates demand from various sources, allowing suppliers to leverage economies of scale, enabling a reduction in costs for proof generation. In turn, the range of use cases that can practically leverage ZKP technology expands – creating a flywheel that grows the aggregate demand for proofs, and hence enables further economies of scale to lower costs. This flywheel makes the economics of ZKPs viable across a much broader range of use cases. When combined with Fermah's several technical breakthroughs, Fermah enables the first efficient marketplace for ZK proof generation.

Roderik van der Graaf, Founder and Managing Partner of Lemniscap, said: "Lemniscap is firmly behind Fermah in their mission to provide fast, cheap, and reliable infrastructure to help developers build category-leading products. By abstracting ZKP complexity, Fermah is lowering the technical barriers to entry, enabling more developers and businesses to integrate these proofs into their systems. This long awaited democratization of ZKPs extends the reach of these advanced cryptographic techniques to a broader range of applications."

Vanishree Rao, Founder and CEO of Fermah, said: "I'm extremely optimistic that Fermah will revolutionize the ZK space as we know it. With the right team, backers, and experience, we're poised to bring our vision to fruition. Soon, incorporating zero knowledge into applications will be frictionless. After over 15 years of building ZKPs, I can clearly see that we are approaching an inflection point: the infrastructure is finally in place, and we're on the precipice of a boom in innovative ZK applications. Fermah will play an integral role in this boom."

About Fermah

Fermah is the universal proof generation layer. It functions as a marketplace, where the supply side comprises GPUs and FPGAs. On the demand side, Fermah can generate proofs for any instance in which ZK is used. Fermah is optimized for cheap, fast, and reliable ZK proof generation.

About Lemniscap

Lemniscap is an investment firm specializing in investments in emerging crypto assets and blockchain startups. Since its founding in 2017, Lemniscap has funded multiple investments in the crypto blockchain space, on the core belief that blockchain technology will upend traditional business models, resulting in profound changes in the world economy. The Lemniscap team consists of talented people with backgrounds in financial markets, PE/VC, technology and entrepreneurship. For more information, visit **https://lemniscap.com/**.

Photo: **https://mma.prnewswire.com/media/2506129/Fermah.jpg**

View original content to download multimedia:**https://www.prnewswire.com/news-releases/fermah-closes-5-2m-seed-round-to-abstract-away-the-complexity-of-zk-proof-generation-302249050.html**

SOURCE Fermah