

Blockchain technology has played a pivotal role in the development of Zero-Knowledge Proofs (ZKPs). So, ZKPs have been widely adopted within the blockchain space to enhance privacy and scalability. However, the potential of ZKPs extends far beyond just the realm of blockchain. In the modern landscape, ZKPs hold immense promise in revolutionizing diverse areas like the Internet of Things (IoT) and Virtual Reality (VR), etc.

zkMIPS

The zkMIPS project leverages the MIPS instruction set to build an efficient ZK VM. The complete zkMIPS whitepaper can be accessed at [zkMIPS whitepaper](#). A succinct overview of the primary approach taken by this project is presented in the next paragraph.

zkMIPS includes a VM capable of executing MIPS programs and interacting with the execution environment, demonstrating its compatibility with diverse platforms. zkMIPS converts the Ethereum Geth into MIPS instruction set and executes the generated program using its VM.

Proof Generation

zkMIPS generates a ZK proof for the resulted execution trace using the state-of-art mechanisms including Starky and Plonky2. An overview version of this architecture can be found in the paper and the proof generation architecture is shown below:

[

ZKMArch

2116×988 196 KB

](<https://ethresear.ch/uploads/default/original/2X/a/ae5e8be40f2b3f6f3a7e00e74087c8cc52cfe3b7.png>)

Proof Size vs. Prover Time

The aim is to design a ZKP system that achieves both a short proof size

, ensuring minimal data overhead, and reduces prover time

to expedite transaction processing. While acknowledging other performance metrics, such as maximum memory usage

, CPU usage

, and the number of constraints

, zkMIPS is committed to optimizing these key aspects to create an efficient and scalable solution. The zkMIPS proof generation process applies the composition and recursion steps to generate a shorter proof obtained in a certain time as required by the target application and hence, strikes a balance between proof size and prover time.

The zkMIPS team requests your valuable feedback, as your insights will be highly appreciated and instrumental in enhancing the project.