Zero-Knowledge Virtual Machines (zkVMs) are specialized virtual machines designed to execute programs while preserving data privacy through zero-knowledge proofs.

A visual representation of zkVM's main components and their interactions can be seen below.

[

image

1500×650 80.3 KB

](https://ethresear.ch/uploads/default/original/2X/8/85426ea778d6cea1fbfb4f6989697a20a199bee7.jpeg)

Current zkVM designs prioritize SNARK compatibility, which in principle requires the minimization of the complexity of the circuit representation of their instructions.

Optimizing for SNARK compatibility does enhance the efficiency of the zero-knowledge proof process, but this often involves using a simplified instruction set. Such simplification inherently constrains the zkVM's capabilities and expressiveness.

Yet, two recent innovations in zkVM optimization techniques are challenging the way we approach zkVM design; Jolt and Lasso.

- Jolt (Just One Lookup Table)

: Introduces a new front-end technique that can be applied to a variety of instruction set architectures. Instead of converting each instruction directly into corresponding arithmetic circuits, Jolt represents these instructions as lookups into pre-determined tables. This provides a considerable efficiency boost because fetching a precomputed value from a table is usually much faster than performing a complex computation.

- Lasso

: Introduces a new lookup argument that uses a predefined table, enabling provers to commit to vectors and ensuring that each entry can be mapped back to this table. This provides an optimization for multiplications-based commitment schemes, creating a dramatically faster prover.

Jolt uses Lasso to offer a new framework for designing SNARKs for zkVMs, and together they can improve performance, developer experience, and auditability for SNARKs

, thus expanding the horizon for zkVM design.

Thank you to the ZKM research team for valuable discussions.