

The Sin7Y team is excited to announce our research and work on designing a ZKVM in our Whitepaper for OlaVM.

The complete Whitepaper is attached at <https://olavm.org/>

#### Abstract:

We designed the architecture for OlaVM, a customized ZKVM, with ambitions to become fully compatible with the existing Ethereum ecosystem, providing seamless migration for projects, enabled at compiler level rather than circuit constraint level. The OlaVM instruction set design strikes a graceful balance between trade-offs in execution trace size and amount of constraints. Utilizing a register-based VM, the overall execution traces of OlaVM are much smaller than that of a stack-based VM. The design of OlaVM revolves around the following main features: (1) A custom virtual machine with a simplified instruction set designed to improve the execution process and ZK verification. (2) Register-based structure, which greatly reduces memory access overhead during the execution process, effectively reducing the scale of the entire execution trace. (3) Finite Field Word, the Word of OlaVM is a field element, the only type of computations that can be performed are field operations, which enables OlaVM to obtain a set of concise state transition constraints. (4) Modular design, dividing the entire execution trace into multiple sub traces based on operation type and processing them separately. (5) FPGA acceleration, utilizing the FPGA acceleration logic of the main calculation module of the ZK algorithm. (6) Zero Knowledge without FFT, eliminating the most computationally expensive module, FFT, in implementing ZK calculations on FPGAs. (7) Other tricks, improving computational efficiency of OlaVM, and of ZK verification through non-deterministic features.

We are proceeding with further research on compatibility with other public blockchains which will be published in a subsequent Yellow Paper, including compatibility with various tooling used by developers amongst other.

If you are interested in our work please check out our [GitHub](#) or reach out to us through Twitter or Telegram. Restriction on links at ethresear.ch, contact details found at our Github. We are looking forward to the community feedback!