ZKWASM-Book

Copy

This repo contains documentation about the ZKWASM and can be seen live at: See the book live ↗.

The mission of DelphiusLab is to provide Web2 developers with a concise toolset to leverage the power of Web3 in their applications. The ZKWASM (ZKSNARK virtual machine that supports Web Assembly) serves as a trustless layer between rich applilcations running on WASM runtime and smart contracts on chain.

WASM (or WebAssembly) is an open standard binary code format similar to assembly. Its initial objective was to provide an alternative to java-script with improved performance for the current web ecosystem. Benefiting from its platform independence, front-end flexibility (can be compiled from the majority of languages including C, C++, assembly script, rust, etc.), good isolated runtime and speed comes closer to the speed of a native binary, its usage is arising in distributed cloud and edge computing. Recently it has become a popular binary format for users to run customized functions on AWS Lambda, Open Yurt, AZURE, etc.

CRYP2NOVA

Archived copy · cryp2nova.com

The idea of ZKWASM is derived from ZKSNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) which is a combination of SNARG (Succinct non-interactive arguments) and zero-knowledge proof. In general, the adoption of ZKSNARK usually requires implementing a program in arithmetic circuits or circuit-friendly languages (Pinocchio, TinyRAM, Buffet/Pequin, Geppetto, xJsnark framework, ZoKrates) that forms a barrier for existing programs to leverage it's power. An alternative approach is, instead of applying ZKSNARK on the source code, applying it on the bytecode level of a virtual machine and implementing a zksnark-backed virtual machine. In this work, we take the approach of writing the whole WASM virtual machine in ZKSNARK circuits so that existing WASM applications can benefit from ZKSNARK by simply running on the ZKWASM, without any modification. Therefore, the cloud service provider can prove to any user that the computation result is computed honestly and no private information is leaked.

Docs include tutorials for the following audiences

1. beginners to get familiar with developping WASM based applications that runs in ZKWASM virtual machine and specifications for zkWASM host circuits.
2. sophisicated rollup application builders that would like to leverage the ability fo ZKWASM for their own application rollup.
3. circuit integrators that would like to use WASM as a glue languague to connect different ZKP circuits for more customizable scenarios (eg. ML, ORACL, VRF, etc)
4. ZKVM builders that would like to use a core minimal set of WASM bytecode to build their own ZK virtual machine.

This document also provides the information regarding the ZKP circuit disign, proof batching and aggregation, proof structure of continuation execution, WASM host circuit integration and WASI support.

This book is a WIP and being constantly updated.

Next
ZKWASM for beginners

Archived copy · cryp2nova.com

Last updated 2 years ago

Archived copy · cryp2nova.com