qedit

ZKPROOF

zkEVM
Formal
Verification
Project

The Verified Verifier

March 2025, ZKProof 7

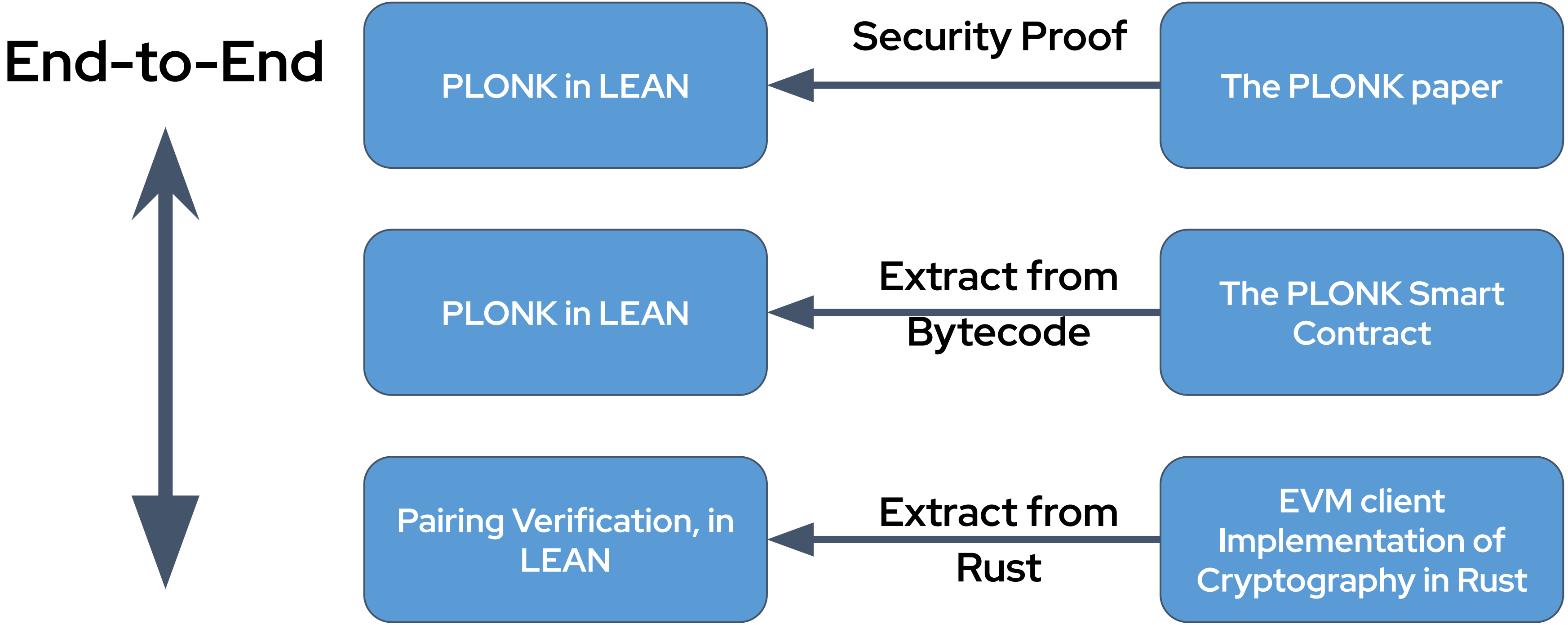
Jonathan Rouach
Executive Director, ZKProof.org
CEO, co-founder, QEDIT

We’re building an end-to-end proof for PLONK verification on Ethereum, using LEAN

- The highest stakes for industry are in zkEVMs
- The most common last step of zkEVM is wrapping for on-chain verification using PLONK / Groth16
- EF is running the largest FV effort today, uses LEAN and targets PLONK, rust

zkEVM
Formal
Verification
Project

With a backbone in Lean from the PLONK paper, we want to show implementation are correct



End-to-End

PLONK in LEAN ← Security Proof ← The PLONK paper

PLONK in LEAN ← Extract from Bytecode ← The PLONK Smart Contract

Pairing Verification, in LEAN ← Extract from Rust ← EVM client Implementation of Cryptography in Rust

Standardizing the Verified Verifier

- Obtain the blessing of the Steering Committee, Standards Committee
- Create the playbook for a secure verifier
- Ready for other schemes