



FORMAL LAND

EQUIVALENCE REVM PYTHON

JUNE 3RD 2024





1 REVM

- Rust version of the EVM
- To be used for ZK versions of the EVM
- 20,000 lines
- <https://github.com/bluealloy/revm>



1 REVM - PROOF

1. **coq-of-rust:** raw version from the source
2. **Linking:** typing and name/trait resolution
3. **Simulation:** idiomatic Coq version
4. **Equivalence:** proof that 2. and 3. run the same



2 PYTHON

- Python version of the EVM
- Used as a reference and sandbox
- 30,000 lines (includes duplicates for versions)
- <https://github.com/ethereum/execution-specs>



2 PYTHON - PROOF

1. **coq-of-python:** raw version from the source
2. **Simulation:** idiomatic Coq version
3. **Equivalence:** proof that 1. and 2. run the same



3 EQUIVALENCE

- Equality between the two EVM versions
- Shown for the simulations
- The Python’s EVM is “included” in Revm
- Python to Revm is surjective
- Might be hard for the environment

THANKS