Examples of proof projects

There are various parts in the protocol which are worth verifying. Some examples are:

1. The encodings. We use the encodings to translate values in binary or JSON format, to save data on the disk or communicate in the RPCs.

2. The Michelson interpreter. This is an optimized interpreter to execute smart contracts, programs which we can also formally verify in Coq.

3. The storage system. The storage system defines high-level abstractions over a more low-level key-value store. Stored values contain various implicit invariants.

Website

Visit the website of our project on:

nomadic-labs.gitlab.io/coq-tezos-of-ocaml

Community

tezos.com
coq.inria.fr
nomadic-labs.com
formal.land

Originated at Nomadic Labs

At Nomadic Labs, we have worked for two years on the project Coq Tezos of OCaml to make a safer code for Tezos. Before that, we initiated the coq-of-ocaml project at Inria and Paris 7.
We continue these ideas with the company Formal Land to bring formal verification to everyday-life programs.

COQ TEZOS OF OCAML

What

A formal approach

We use the formal proof system Coq to mathematically verify that our code does what it is intended to do. Mistakes are virtually impossible.

Pipeline

We translate the OCaml code of Tezos into a similar-looking Coq code, using the coq-of-ocaml translator.

Specify

We can either write specifications directly in Coq, or in the OCaml code with assertions or boolean properties.

Verify

We write the proofs in Coq, using a manual or automated style. Doing so, we make sure that our properties are valid for all possible inputs.

SPECIFY.
VERIFY.
BE SURE.

COQ
TEZOS
OF
OCAML

Operators in Michelson: A Visitor Guide

During the development process, we detected an issue in the new implementation of the comparison operator for Michelson values.

We wrote property-based tests to make sure no regressions were possible after fixing the issue. In addition to that, we decided to formally specify and verify the comparison operator. The code is not entirely trivial, as we wrote it in a continuation-passing style. In the specification, we explicit that the comparison is a preorder because signatures can appear in different and non-distinguishable formats.